S.No.	RFP Section	Sub-Section	Pg No	RFP Clause	Bidder Query	LIC Response
				Life Insurance Corporation of India – RFP/Tender for onboarding System Integrator (SI) to Implement Network Security Tools - Response to Pre-bid Queries (LIC-CO/IT-BPR/NW/RFP/2023-2024/NS dated 06 February 2024)		
1	-	-	Additional point (must have)	The SSLO devices should be STIP compliant.	STIP compliance is part of Common Criteria (CC) that provides a common set of requirements for the security functionality of IT products and the assurance measures to be applied to the IT products during a security evaluation. Does LIC require the SSLO device to be STIP compliant?	Please be guided by the RFP
2	-	-	Additional Query		Kindly confirm the total number of applications to be considered for onboarded on SSLO during the deployment phase.	Please be guided by the RFP
3	Annexure F - Technical Compliance	API GW	13	The solution should provide features to Convert between different data formats (e.g., JSON to XML).	We request LIC to reconsider older protocol supports like XML is an outdated API protocol, also JSON to XML translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The solution should provide seamless integration with additional package to Convert between different data formats (e.g., JSON to XML) without adding overheads API-GW solution."	API Gateway and Security Solution has been removed from the scope of this RFP
4	Annexure F - Technical Compliance	API GW	19	The proposed solution should facilitate seamless SOAP to REST transformation, enabling interoperability by translating SOAP-based requests into RESTful API calls, promoting modern integration practices.	We request LIC to reconsider older protocol supports like SOAP is XML based outdated API protocol, also SOAP (XML) to REST (JSON) translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The proposed solution should seamless integration with additional package to translate SOAP to REST, enabling interoperability by translating SOAP-based requests into RESTful API calls as and when required without adding overheads API-GW solution, promoting modern integration practices".	API Gateway and Security Solution has been removed from the scope of this RFP
5	Annexure F - Technical Compliance	API GW	20	The solution should be designed to facilitate a developer organization by providing comprehensive tools, documentation, and support for efficient development.	We request LIC to consider that the mentioned features are getting fulfilled with development tools, not by API gateway, introducing it on API GW will increase overhead and it force developer to restrict themselves to limited features available on such tool. We request LIC to change this clause as: "The solution should be designed to facilitate to integrate it with developer organization by providing compatibility with multiple tools and support for efficient development with the Security of authentication, authorization, payload sanitization and WAF signature inspection"	API Gateway and Security Solution has been removed from the scope of this RFP
6	Annexure F - Technical Compliance	API GW	31	The API gateway should implement streaming APIs using compatible protocols like WebSocket, WebSub, or server-sent events.	We request LIC to kindly change this clause as web-Sub is a protocol usually used to push content by many websites, including all blogs served by Blogger and WordPress.com news sites. This use case seems to be irrelevant to LIC. Recommended revised clause: "The API gateway should implement streaming APIs using compatible protocols like WebSocket and server-sent events and support Web-Sub via plugins/packages."	API Gateway and Security Solution has been removed from the scope of this RFP
7	Annexure F - Technical Compliance	WAF Technical specs DC-DR	17	The proposed solution must support 10 Gbps of WAF throughput with minimum 128GB RAM. In case any OEM/bidder has WAF and load balancer in same appliance then the total L7 throughput should at least be 200Gbps with minimum 192GB RAM or more. The bidder must provide evidence of throughput through publicly available documents at OEM websites prior to the date of RFP	We request LIC to clarify the requirement of 10 Gbps WAF, is this HTTP or HTTPs throughput ? The difference is that when WAF devices does decryption as is the rightly the ask of the RFP it should publish numbers for HTTPs and not HTTP on the Public datasheet.	WAF throughput must meet a minimum of 10Gbps as outlined in the datasheet, specifically for HTTPS traffic. However, if the term "WAF throughput" is not explicitly stated in the datasheet, then the Layer 7 throughput should be 200Gbps or higher for HTTPS traffic.
8	Annexure F - Technical Compliance	WAF Technical specs DC-DR	19	The Proposed WAF should support 10 Gbps of WAF throughput and minimum 30000 RSA Per SEC (2048 BIT)/ECC.	We request LIC to clarify the requirement of 10 Gbps WAF, is this HTTP or HTTPs throughput ? The difference is that when WAF devices does decryption as it is rightly asked in the RFP it should publish numbers for HTTPs and not HTTP on the datasheet	WAF throughput, as stated in the datasheet, must reach 10Gbps, specifically for HTTPS traffic. However, if the term "WAF throughput" is not explicitly stated in the datasheet, then the L7 throughput should be 200Gbps or higher for HTTPS traffic.
9	Annexure F - Technical Compliance	WAF Technical specs DC-DR	98	The solution should be able to block even the most advanced bots that try to emulate standard client behaviour and pretend to be web browsers.	Is LIC looking at Cloud based BOT mitigation service or on prem?	The WAF must be deployed on-premises as a hardware appliance, equipped with the capability to detect bots directly on the device. However, for more sophisticated bots, the WAF must include a feature to conduct additional inspection in the cloud, utilizing the same license. The integration between the WAF and the cloud-based bot engine must be seamless, ensuring that only header information is transmitted to the cloud-based bot for inspection, while the payload remains within the WAF and is not sent to the cloud-based bot engine.
10	Annexure F - Technical Compliance	WAF Technical specs DC-DR	98	The solution should be able to block even the most advanced bots that try to emulate standard client behaviour and pretend to be web browsers.	We request LIC to clarify if 1M transactions/day would suffice the requirement for licensing of BOT solution.	Please be guided by the RFP
11	Annexure F - Technical Compliance	WAF Technical specs DC-DR	108	The system should provide the ability to apply the following actions against traffic classified as BOT: 1. Blocking 2. Monitoring 3. Displaying a Captcha 4. Identify 5. Delay	We request LIC to remove the delay clause, as mitigation action it is not recommended to allow any kind of malicious actor to access the website, delaying will not help to protect against web scraping and data leakages. We request LIC to revise the clause as below: The system should provide the ability to apply the following actions against traffic classified as BOT: 1. Blocking 2. Monitoring 3. Displaying a Captcha 4. Identify	Please be guided by the RFP
12	Annexure F - Technical Compliance	WAF Technical specs DC-DR	111	Part of the product should be a flexible reporting system that can generate detailed views, including: 1. Applied actions on the timeline 2. Number of solved/unsolved captcha 3. The performance of ML models 4. The incidence of customer anomalies 5. Ratio of bad bot/good bot/human traffic 6. Endpoints with the highest number of requests.	We request LIC to delete ask of performance of ML models and number of solved captcha the end goal of an anti-bot solution should be to offer granule visibility into device types, geolocations of attackers, fingerprints of attackers, % of humans vs Bots & blocked vs Allowed transactions etc. We request LIC to modify clause as below: Part of the product should be a flexible reporting system that can generate detailed views, including: 1. Applied actions on the timeline 2. The incidence of customer anomalies 3. Ratio of bad bot/good bot/human traffic 4. Endpoints with the highest number of requests.	Please be guided by the RFP
13	Annexure F - Technical Compliance	WAF Technical specs DC-DR	114	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure	We request LIC to delete this clause and to consider the ramifications of hardware bypass and to run application exposed to security threats during run time. LIC is investing in high availability devices with aggressive RMA SLA's hence we recommend using HA failover capabilities so that even during failure of devices or software the application can still be protected	Please be guided by the RFP

14	Annexure F - Technical Compliance	WAF Technical specs DC-DR	115	The proposed WAF appliance MUST NOT USE Hypervisors. The appliance must be a purpose built WAF with its own custom specialised hardened OS integrated with the hardware. It must not have any Virtualisation components in the hardware.	We request LIC to delete this clause, as each OEM has different engineering architecture, moreover without hypervisor LIC will lose the ability to create vWAF's for micro segmentation and ease of operations. Virtualization offers below benefits: 1. Micro segmentation 2. control on usage of resources 3. OS upgrades without affecting other tenants 4. if LIC wishes to emulate the bare metal functions just create single large tenant with all resources. There is no known advantage of running without hypervisors and this ask seems irrelevant	Please be guided by the RFP
15	Annexure F - Technical Compliance	WAF Technical specs NDR	17	The proposed solution must support 10 Gbps of WAF throughput with minimum 128GB RAM. In case any OEM/bidder has WAF and load balancer in same appliance then the total L7 throughput should at least be 200Gbps with minimum 192GB RAM or more. The bidder must provide evidence of throughput through publicly available documents at OEM websites prior to the date of RFP	We request LIC to clarify the requirement of 10 Gbps WAF, is this HTTP or HTTPs throughput ? The difference is that when WAF devices does decryption as is the rightly the ask of the RFP it should publish numbers for HTTPs and not HTTP on the Public datasheet.	WAF throughput must meet a minimum of 10Gbps as outlined in the datasheet, specifically for HTTPS traffic. However, if the term "WAF throughput" is not explicitly stated in the datasheet, then the Layer 7 throughput should be 200Gbps or higher for HTTPS traffic.
16	Annexure F - Technical Compliance	WAF Technical specs NDR	19	The Proposed WAF should support 10 Gbps of WAF throughput and minimum 30000 RSA Per SEC (2048 BIT)/ECC.	We request LIC to clarify the requirement of 10 Gbps WAF, is this HTTP or HTTPs throughput ? The difference is that when WAF devices does decryption as it is rightly asked in the RFP it should publish numbers for HTTPs and not HTTP on the datasheet	Please be guided by the RFP
17	Annexure F - Technical Compliance	WAF Technical specs NDR	86	The solution must protects system against WASC Web Security Attack classification.	We request LIC to remove this point as WASC is outdated consortium the release was 12 years back. OWASP top 10 should be considered instead as it covers the latest attack types.	Please refer to the revised "Annexure F"
18	Annexure F - Technical Compliance	WAF Technical specs NDR	98	The solution should be able to block even the most advanced bots that try to emulate standard client behaviour and pretend to be web browsers.	We request LIC to clarify if 1M transactions/day would suffice the requirement for licensing of BOT solution.	Please be guided by the RFP
19	Annexure F - Technical Compliance	WAF Technical specs NDR	108	The system should provide the ability to apply the following actions against traffic classified as BOT: 1. Blocking 2. Monitoring 3. Displaying a Captcha 4. Identify 5. Delay	We request LIC to remove the delay clause, as mitigation action it is not recommended to allow any kind of malicious actor to access the website, delaying will not help to protect against web scraping and data leakages. We request LIC to revise the clause as below: The system should provide the ability to apply the following actions against traffic classified as BOT: 1. Blocking 2. Monitoring 3. Displaying a Captcha 4. Identify	Please be guided by the RFP
20	Annexure F - Technical Compliance	WAF Technical specs NDR	111	Part of the product should be a flexible reporting system that can generate detailed views, including: 1. Applied actions on the timeline 2. Number of solved/unsolved captcha 3. The performance of ML models 4. The incidence of customer anomalies 5. Ratio of bad bot/good bot/human traffic 6. Endpoints with the highest number of requests.	We request LIC to delete ask of performance of ML models and number of solved captcha the end goal of an anti-bot solution should be to offer granule visibility into device types, geolocations of attackers, fingerprints of attackers, % of humans vs Bots & blocked vs Allowed transactions etc. We request LIC to modify clause as below: Part of the product should be a flexible reporting system that can generate detailed views, including: 1. Applied actions on the timeline 2. The incidence of customer anomalies 3. Ratio of bad bot/good bot/human traffic 4. Endpoints with the highest number of requests.	Please be guided by the RFP
21	Annexure F - Technical Compliance	WAF Technical specs NDR	114	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure	We request LIC to delete this clause and to consider the ramifications of hardware bypass and to run application exposed to security threats during run time. LIC is investing in high availability devices with aggressive RMA SLA's hence we recommend using HA failover capabilities so that even during failure of devices or software the application can still be protected	Please be guided by the RFP
22	Annexure F - Technical Compliance	WAF Technical specs NDR	115	The proposed WAF appliance MUST NOT USE Hypervisors. The appliance must be a purpose built WAF with its own custom specialised hardened OS integrated with the hardware. It must not have any Virtualisation components in the hardware.	We request LIC to delete this clause, as each OEM has different engineering architecture, moreover without hypervisor LIC will lose the ability to create vWAF's for micro segmentation and ease of operations. Virtualization offers below benefits: 1. Micro segmentation 2. control on usage of resources 3. OS upgrades without affecting other tenants 4. if LIC wishes to emulate the bare metal functions just create single large tenant with all resources. There is no known advantage of running without hypervisors and this ask seems irrelevant	Please be guided by the RFP
23	Onsite Support Services:	III. SSL Off Loader	Page 58	The SSL off loader should be from a different OEM than WAF	Request LIC to relax this clause, the entire industry is focusing on consolidation of vendors/services to avoid multiple tools sprawl. The management and day-2 activity including patching and operations becomes easy if single OEM can cater to multiple solutions. Following are the benefits of single OEM having consolidation across products 1. No need for separate skills sets of people on WAF and SSLO 2. Single ownership with one OEM - less people to co-ordinate 3. max interoperability between SSLO and WAF - no surprises for technical interoperability 4. This clause is restrictive and will not allow vendors like Citrix, Radware, Array to participate for WAF and SSLO	Please be guided by the RFP
24	Annexure F - Technical Compliance	WAF Technical specs DC-DR	17	The proposed solution must support 10 Gbps of WAF throughput with minimum 128GB RAM. In case any OEM/bidder has WAF and load balancer in same appliance then the total L7 throughput should at least be 200Gbps with minimum 192GB RAM or more. The bidder must provide evidence of throughput through publicly available documents at OEM websites prior to the date of RFP	Please clarify, is this HTTP or HTTPs throughput ?	WAF throughput must meet a minimum of 10Gbps as outlined in the datasheet, specifically for HTTPS traffic. However, if the term "WAF throughput" is not explicitly stated in the datasheet, then the Layer 7 throughput should be 200Gbps or higher for HTTPS traffic.
25	Annexure F - Technical Compliance	WAF Technical specs DC-DR	19	The Proposed WAF should support 10 Gbps of WAF throughput and minimum 30000 RSA Per SEC (2048 BIT)/ECC.	Please clarify, is this HTTP or HTTPs throughput ?	Please be guided by the RFP
26	Section C	Anexxure R	19		Quantity of WAF gateways and Management systems are not mentioned in Annexure R Bill of Quantity	Please refer to the revised "Annexure G"

#	Section	Sub	Clause	Clause Text	Request / Query	Response
27	Section H	Annexure F, 10		For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authentcated via RADIUS, TACACS+ or via local tabel of authorized users.	Request to modify the clause as "For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authentcated via RADIUS/ TACACS+ / via local table of authorized users."	Please refer to the revised "Annexure F"
28	Section H	Annexure F, 86		The solution must protect system against WASC Wec Security Attack classification.	Request to modify the clause as "The solution must protect system against WASC Wec Security Attack classification or OWASP top 10."	Please refer to the revised "Annexure F"
29	Compliance			The CASB Solution must have HTTP/2 support from day 1.	This is Web Security (SWG) feature. It is requested to remove this clause.	Please refer to the revised "Annexure F"
30	Compliance			The CASB Solution must have 99% uptime SLA	Considering business applications access via Cloud Service provider,SLA's for Cloud Vendor has to high. Our request to consider 99.999% uptime SLA instead of 99%	Please refer to the revised "Annexure F"
31	Compliance			The solution must have Web IPS (Signatures) to protect against targeted user-agent threats	This is SWG feature and not CASB feature. CASB is meant to protect SaaS applications and not vulnerabilities.This need SWG license consideration. Kindly relax the point.	Please refer to the revised "Annexure F"
32	Annexure F - Technical Compliance	NAC Technical Specificatio n	65	The Proposed solution must have atleast 64GB RAM	Different Solution have various RAM requirement , for such a large requirement (1,27,000 endpoints), 64GB RAM may cause overall solution performance related issues. Request you to modify the clause as "The Proposed solution must have appropriate RAM so the overall solution will provide optimal performance across LIC network."	A minimum of 64GB RAM is required . However , the bidders may size it more as per the requirement .
33	Annexure F - Technical Compliance	NAC Technical Specificatio n	67	The Proposed solution should provide comprehensive visibility of the network by automatically discovering, classifyting, and enforcing policy for the endpoints connected to the network and must have capacity to enable the appropriate services for the total 1,27,000 endpoint devices scalable to 1,60,000 devices	LIC need 1,27,000 enpoint devices licenses and corresponding Hardware from day 1 and LIC will add additinoal Licenses and Hardware as and when require to meet the scalability of 1,60,000 devices, Does our understanding is correct?	The hardware has to be sized for 1,60,000 devices from day one . However , LIC may place the purchase order for the licenses in a staggered manner.
34	Annexure F - Technical Compliance	NAC Technical Specificatio n	68	The Proposed solution should support on-demand Health-check of the hardware nodes	NAC solution must support out of box monitoring dashboard for all NAC HW like CPU load , Device HDD , Device managed endpoints , Total Memory , Appliance traffic etc. Does our understanding is correct?	Please be guided by the RFP
35	Annexure F - Technical Compliance	NAC Technical Specificatio n	74	The Proposed Solution must support agent based and Agent less based approach	The NAC solution should support agentbased and agentless mode to achieve all feature & functionality which includes device visibility , Authentication, classification , Posture accessment , Remediations , Control and Automation, Does our understanding is correct?	Please be guided by the RFP
36	Annexure H: Manufacturer's Authorization Form (MAF)		121	_____ (OEM) certify that, the equipments being sold would not be declared End of Support (EoS) in the next 6Years and that _____ (OEM) shall supply suitable substitute in case EoS of equipments. Also _____ (OEM) certifies that the products being sold would be covered under Warranty / Support and support will be available for next six years (five years initially and one year if extension is provided) from the date of installation at LIC of India.	Requesting LIC to change the no of years from 6 years to 5 years only for EOS and also from Support point of view. Most of the securuty solution "appliance" life is not more than 5 years. Hence request you to limit the years to 5 only.	Please refer to the revised "Annexure H"
37	Additional Points			Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , IP Printers , IP Scanners etc.- IoT (IP Printer , IP Scanner , IP Phone , IP camera etc) Risk Assessment such as -- Detect Unsecure (TCP/UDP port open (For example IP camera having Telnet Port open etc) -- Detect IOT's devices using factory default or Weak/common credentials for SNMP/SSH/TELNET.	Requesting LIC to consider the point since LIC will have ~30% IOT devices which will not support traditional authentication method (such as Radius/Dot1X). It is not a good idea to only depend on 802.1x/MAC address bypass. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. Also MAC address repository should be uptodate at any point in time to meet security aspect.	Please refer to the revised "Annexure F"
38	Additional Points			The NAC solution should support agentless mode to achieve all feature & functionality which includes device visibility , Authentication, classification , Posture accessment , Remediations , Control and Automation	It is important to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible.	Please be guided by the RFP
39	Additional Points			Solution must support various controls based on compliance requirement like Move to Quarantine VLAN , endpoint ACL/Port ACL/Switch Port block , WLAN block etc via SNMP , CLI based integration with Switches & WLC.	NAC solution must support for various blocking option,according to LIC current environment and future request decision will be made during deployment.	Please be guided by the RFP
40	Additional Points			NAC Solution must identify application change on the endpoint , Host Name change , OS change , Change in shared folder , User change etc & take the control and notification action automatically based on the LIC policy	NAC solution must detect the changes in the endpoints which will helps the LIC to know the actual changes on the endpoint and accordingly LIC can take/modify their compliance for better security.	Please be guided by the RFP
41	Additional Points			NAC solution must support out of box monitoring dashboard for all NAC HW like CPU load , Device HDD , Device managed endpoints , Total Memory , Appliance traffic etc	Since in the RFP it is mentioned LIC is providing the HW for NAC deployment , it is important to know the usage/performance of the HW where NAC solution is deployed this dasboard helps the L1/L2 resource to get alert on the resource consumption and take precautionary measure if their is any Indications/abnormalities.	Please be guided by the RFP
42	Additional Points			Solution Must provide complete device visibility , compliance check , Remediation , blocking and Integration with other security solutions. features for the devices which are not supporting 802.1X Architecture. Proposed solution must achieve the same capability without deploying agent on Windows, MAC Book , Linux, IP Phone , IP camera , IP Printer , IP Scanner etc.	LIC have 100% infrastructure which may not capable to handle full 802.1x capability. It is important for any solution to provide full capability to support existing infrastructure to restrict the non-complient/Rough/Non-LIC endpoint. It will help in faster deployement cycle which rusIt in decreasing overall TCO. **Gartner 2021 Recommendation** Pursue a preconnect or postconnect authentication approach. The preconnect authentication approach can be thought of as a "guilty until proven innocent" model ("default deny"), whereas post connect authentication can be considered an "innocent until proven guilty" model ("default allow"). Preconnect = 802.1x (Fail close) Postconnect = non-802.1x (Fail Safe)	Please be guided by the RFP
43	Additional Points			Solution Must support Non-802.1X Architecture to integratw with existing network infrastructure without the need of any hardware and software upgrades required for 802.1X deployment. Proposed solution must integrate with exisitng Switches/Wireless via SNMP/SSH parameter to block/Isolate the devices.		Please be guided by the RFP
44	Additional Points			The solution should integrate with VM infrastructure to provide out of the box visibility to Virtual Machine properties such as Boot Time, Virtual Machine Hardware, Virtual Machine is Orphan, Virtual Machine Peripheral Devices info, Virtual Machine Port Group, Virtual Machine Power State, Virtual Machine Usage CPU (one thousandth), Virtual Machine Usage Network I/O (KBps), etc. Solution must support multiple auto-remediation methods on Vmware vSpehere like Power On Virtual machine , Power-Off Virtual machine , Reboot Virtual machine , Suspend Virtual machine , Install/Upgrade VM tool based on policy	LIC must have enterprise datacenter deployed over virtual infrastructure. It is always recommend to have detailed perview of all such devices under NAC to avoid any security non-compliance & help in inproving the LIC security.	Please be guided by the RFP

45	Additional Points			Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , IP Printers , IP Scanners etc. IoT (IP Printer , IP Scanner , IP Phone , IP camera etc) compliance : The solution should be able to identify all network devices such as -- Unsecure (TCP/UDP port open (For example IP camera having Telnet Port open etc) -- IOT's devices using factory default or Weak/common credentials for SNMP/SSH/TELNET.	LIC will have ~30% IOT devices which will not support traditional authentication method (such as Radius/Dot1X). It is not a good idea to only depend on MAC address whitelist. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. Also MAC address repository should be uptodate at any point in time to meet security aspect. **Gartner 2021 Recommendation** Gain visibility into on-premises infrastructure-connected devices with the goal of implementing access policies These devices include commonly used ones like workstations, laptops, printers,IP phones, IP cameras, access points, and IoT devices like OT, medical and building automation devices. Often, this motivation is driven by audit findings or an overall security strategy requiring authentication of all devices on a network.	Please refer to the revised "Annexure F"
46	Additional Points			The proposed solution must receive the SIEM data to take policy-based response actions such as quarantining or blocking potentially compromised or noncompliant devices, depending on the severity of the violation information received from SIEM. For example, SIEM detects, via firewall log correlation, a targeted denial of service (DoS) attack, it can direct proposed solution to have the the firewall automatically block the source of the attack to prevent further disruption of service to the application(s) on the network.	**Gartner 2021 Recommendation** Enable interoperability with other security solutions. This can be achieved in two ways: customization through open APIs or the use of built-in integration. NAC solutions increasingly feature anomaly detection capability to detect infected endpoints and MAC spoofing attempts on a network. However, integration with other security tools creates a better overall security context for an organization, which can be used to respond automatically to infected endpoints by quarantining them and thus preventing the spread of malware.	Please refer to the revised "Annexure F"
47	Additional Query				Please share total number of Network/L2-L3 devices i.e. Switches , Routers , Access Points , WLC , Firewall etc.	The details shall be shared with the successful bidder
48	Additional Points			Proof of Concept (POC) in Live enviroment The LIC at its discretion may ask for the Proof-of-Concept/Value (POC/POV) of the proposed solution in the production set up with the bidders whose bids are technically qualified. 1. The LIC will provide a couple of week's time for conducting POC/ POV at LIC's production environment for the solution proposed in the tender. 2. The LIC may raise certain clarifications during evaluation and the respective bidder should provide the response as per timelines stipulated from time to time without which the bid will be treated as incomplete and may be rejected. 3. Failing to comply with the requirements of the LIC as mentioned in the Tender document or if the solution does not fit into the LIC's production setup due to any third party dependencies etc. then the bid will be treated as incomplete and may be rejected.	Live Proof of Concept (POC) is important for Network Access Control (NAC) projects for several reasons: 1. Validation of Functionality: It allows LIC to validate that the proposed NAC solution works as intended in their specific environment. This ensures that the solution meets the LIC's requirements and effectively addresses the security needs. 2. Identification of Challenges: Live POC helps identify any potential challenges or issues that may arise during deployment or operation. This allows for troubleshooting and fine-tuning before full implementation, minimizing disruptions and optimizing performance. 3. Risk Mitigation: Live POC allows organizations to assess the risks associated with implementing a new NAC solution in LIC environment before committing to a full rollout. This proactive approach helps mitigate potential security vulnerabilities and operational risks. Conducting a live POC for a NAC project helps ensure successful deployment, minimize risks, and optimize the solution to meet the organization's specific requirements.	Please refer to the revised "Technical Bid Evaluation"
49	-	-	-	-	With respect to MDM, need a clarity that can proposed solution be on cloud like SaaS offering with data residency in India. IBM MaaS360 is a SaaS Unified Endpoint Management solution offered by IBM that manages and protects any existing endpoint including laptops, desktops, mobile devices and apps, wearables, IoT and purpose built devices and allow protected, low risk access to company resources.	On Prem Solution is required
50	Annexure F - Technical Compliance	NAC Technical Specificatio n	65	The Proposed solution must have atleast 64GB RAM	Different Solution have various RAM requirement , for such a large requirement (1,27,000 endpoints), 64GB RAM may cause overall solution performance related issues. Request you to modify the clause as "The Proposed solution must have appropriate RAM so the overall solution will provide optimal performance across LIC network".	A minimum of 64GB RAM is required . However , the bidders may size it more as per the requirement .
51	Annexure F - Technical Compliance	NAC Technical Specificatio n	67	The Proposed solution should provide comprehensive visibility of the network by automatically discovering, classifyting, and enforcing policy for the endpoints connected to the network and must have capacity to enable the appropriate services for the total 1,27,000 endpoint devices scalable to 1,60,000 devices	LIC need 1,27,000 enpoint devices licenses and corresponding Hardware from day 1 and LIC will add additinoal Licenses and Hardware as and when require to meet the scalability of 1,60,000 devices, Does our understanding is correct?	The hardware has to be sized for 1,60,000 devices from day one . However , LIC may place the purchase order for the licenses in a staggered manner.
52	Annexure F - Technical Compliance	NAC Technical Specificatio n	68	The Proposed solution should support on-demand Health-check of the hardware nodes	NAC solution must support out of box monitoring dashboard for all NAC HW like CPU load , Device HDD , Device managed endpoints , Total Memory , Appliance traffic etc. Does our understanding is correct?	Please be guided by the RFP
53	Annexure F - Technical Compliance	NAC Technical Specificatio n	74	The Proposed Solution must support agent based and Agent less based approach	The NAC solution should support agentbased and agentless mode to achieve all feature & functionality which includes device visibility , Authentication, classification , Posture accessment , Remediations , Control and Automation, Does our understanding is correct?	Please be guided by the RFP
54	Annexure H: Manufacturer's Authorization Form (MAF)		121	_____ (OEM) certify that, the equipments being sold would not be declared End of Support (EoS) in the next 6Years and that _____ (OEM) shall supply suitable substitute in case EoS of equipments. Also _____ (OEM) certifies that the products being sold would be covered under Warranty / Support and support will be available for next six years (five years initially and one year if extension is provided) from the date of installation at LIC of India.	Requesting LIC to change the no of years from 6 years to 5 years only for EOS and also from Support point of view. Most of the securuty solution "appliance" life is not more than 5 years. Hence request you to limit the years to 5 only.	Please refer to the revised "Annexure H"
55	Additional Points			Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , IP Printers , IP Scanners etc.- IoT (IP Printer , IP Scanner , IP Phone , IP camera etc) Risk Assessment such as -- Detect Unsecure (TCP/UDP port open (For example IP camera having Telnet Port open etc) -- Detect IOT's devices using factory default or Weak/common credentials for SNMP/SSH/TELNET.	Requesting LIC to consider the point since LIC will have ~30% IOT devices which will not support traditional authentication method (such as Radius/Dot1X). It is not a good idea to only depend on 802.1x/MAC address bypass. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. Also MAC address repository should be uptodate at any point in time to meet security aspect.	Please refer to the revised "Annexure F"
56	Additional Points			The NAC solution should support agentless mode to achieve all feature & functionality which includes device visibility , Authentication, classification , Posture accessment , Remediations , Control and Automation	It is important to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible.	Please be guided by the RFP
57	Additional Points			Solution must support various controls based on compliance requirement like Move to Quarantine VLAN , endpoint ACL/Port ACL/Switch Port block , WLAN block etc via SNMP , CLI based integration with Switches & WLC.	NAC solution must support for various blocking option,according to LIC current environment and future request decision will be made during deployment.	Please be guided by the RFP
58	Additional Points			NAC Solution must identify application change on the endpoint , Host Name change , OS change , Change in shared folder , User change etc & take the control and notification action automatically based on the LIC policy	NAC solution must detect the changes in the endpoints which will helps the LIC to know the actual changes on the endpoint and accordingly LIC can take/modify their compliance for better security.	Please be guided by the RFP

#	Section	Sub	Pt	Requirement	Query / Justification	Response
59	Additional Points			NAC solution must support out of box monitoring dashboard for all NAC HW like CPU load , Device HDD , Device managed endpoints , Total Memory , Appliance traffic etc	Since in the RFP it is mentioned LIC is providing the HW for NAC deployment , it is important to know the usage/performance of the HW where NAC solution is deployed this dasboard helps the L1/L2 resource to get alert on the resource consumption and take precautionary measure if their is any Indications/abnormalities.	Please be guided by the RFP
60	Additional Points			Solution Must provide complete device visibility , compliance check , Remediation , blocking and Integration with other security solutions. features for the devices which are not supporting 802.1X Architecture. Proposed solution must achieve the same capability without deploying agent on Windows, MAC Book , Linux, IP Phone , IP camera , IP Printer , IP Scanner etc.	LIC have 100% infrastructure which may not capable to handle full 802.1x capability. It is important for any solution to provide full capability to support existing infrastructure to restrict the non-compliant/Rough/Non-LIC endpoint. It will help in faster deployement cycle which ruslt in decreasing overall TCO. **Gartner 2021 Recommendation** Pursue a preconnect or postconnect authentication approach. The preconnect authentication approach can be thought of as a "guilty until proven innocent" model ("default deny"), whereas post connect authentication can be considered an "innocent until proven guilty" model ("default allow"). Preconnect = 802.1x (Fail close) Postconnect = non-802.1x (Fail Safe)	Please be guided by the RFP
61	Additional Points			Solution Must support Non-802.1X Architecture to integratw with existing network infrastructure without the need of any hardware and software upgrades required for 802.1X deployment. Proposed solution must integrate with exisitng Switches/Wireless via SNMP/SSH parameter to block/Isolate the devices.		Please be guided by the RFP
62	Additional Points			The solution should integrate with VM infrastructure to provide out of the box visibility to Virtual Machine properties such as Boot Time, Virtual Machine Hardware, Virtual Machine is Orphan, Virtual Machine Peripheral Devices info, Virtual Machine Port Group, Virtual Machine Power State, Virtual Machine Usage CPU (one thousandth), Virtual Machine Usage Network I/O (KBps), etc. Solution must support multiple auto-remediation methods on Vmware vSpehere like Power On Virtual machine , Power-Off Virtual machine , Reboot Virtual machine , Suspend Virtual machine , Install/Upgrade VM tool based on policy	LIC must have enterprise datacenter deployed over virtual infrastructure. It is always recommend to have detailed perview of all such devices under NAC to avoid any security non-compliance & help in inproving the LIC security.	Please be guided by the RFP
63	Additional Points			Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , IP Printers , IP Scanners etc. IoT (IP Printer , IP Scanner , IP Phone , IP camera etc) compliance : The solution should be able to identify all network devices such as -- Unsecure (TCP/UDP port open (For example IP camera having Telnet Port open etc) -- IOT's devices using factory default or Weak/common credentials for SNMP/SSH/TELNET.	LIC will have ~30% IOT devices which will not support traditional authentication method (such as Radius/Dot1X). It is not a good idea to only depend on MAC address whitelist. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. Also MAC address repository should be uptodate at any point in time to meet security aspect. **Gartner 2021 Recommendation** Gain visibility into on-premises infrastructure-connected devices with the goal of implementing access policies These devices include commonly used ones like workstations, laptops, printers,IP phones, IP cameras, access points, and IoT devices like OT, medical and building automation devices. Often, this motivation is driven by audit findings or an overall security strategy requiring authentication of all devices on a network.	Please be guided by the RFP
64	Additional Points			The proposed solution must receive the SIEM data to take policy-based response actions such as quarantining or blocking potentially compromised or noncompliant devices, depending on the severity of the violation information received from SIEM. For example, SIEM detects, via firewall log correlation, a targeted denial of service (DoS) attack, it can direct proposed solution to have the the firewall automatically block the source of the attack to prevent further disruption of service to the application(s) on the network.	**Gartner 2021 Recommendation** Enable interoperability with other security solutions. This can be achieved in two ways: customization through open APIs or the use of built-in integration. NAC solutions increasingly feature anomaly detection capability to detect infected endpoints and MAC spoofing attempts on a network. However, integration with other security tools creates a better overall security context for an organization, which can be used to respond automatically to infected endpoints by quarantining them and thus preventing the spread of malware.	Please refer to the revised "Annexure F"
65	Additional Query				Please share total number of Network/L2-L3 devices i.e. Switches , Routers , Access Points , WLC , Firewall etc.	The details shall be shared with the successful bidder
66	Additional Points			Proof of Concept (POC) in Live enviroment The LIC at its discretion may ask for the Proof-of-Concept/Value (POC/POV) of the proposed solution in the production set up with the bidders whose bids are technically qualified. 1. The LIC will provide a couple of week's time for conducting POC/ POV at LIC's production environment for the solution proposed in the tender. 2. The LIC may raise certain clarifications during evaluation and the respective bidder should provide the response as per timelines stipulated from time to time without which the bid will be treated as incomplete and may be rejected. 3. Failing to comply with the requirements of the LIC as mentioned in the Tender document or if the solution does not fit into the LIC's production setup due to any third party dependencies etc. then the bid will be treated as incomplete and may be rejected.	Live Proof of Concept (POC) is important for Network Access Control (NAC) projects for several reasons: 1. Validation of Functionality: It allows LIC to validate that the proposed NAC solution works as intended in their specific environment. This ensures that the solution meets the LIC's requirements and effectively addresses the security needs. 2. Identification of Challenges: Live POC helps identify any potential challenges or issues that may arise during deployment or operation. This allows for troubleshooting and fine-tuning before full implementation, minimizing disruptions and optimizing performance. 3. Risk Mitigation: Live POC allows organizations to assess the risks associated with implementing a new NAC solution in LIC environment before committing to a full rollout. This proactive approach helps mitigate potential security vulnerabilities and operational risks. Conducting a live POC for a NAC project helps ensure successful deployment, minimize risks, and optimize the solution to meet the organization's specific requirements.	Please refer to the revised "Technical Bid Evaluation"
67	Section E: Scope of Services	Implementation - point 3	51	The bidder is responsible for determining the appropriate hardware sizing. LIC will supply the server, rack space, and cooling. The bidder is also responsible for furnishing any other necessary hardware or equipment to ensure smooth integration of all the in-scope solutions. As per LIC's requirement, the successful bidder of the project shall be ready to shift, occasionally, the equipment from one place to other, uninstall and reinstall all the equipment without any additional cost to LIC.	Our understanding is LIC will provide the underlying infra, hypervisor, OS and db. Kindly confirm	Please be guided by the RFP
68	Section E: Scope of Services	Implementation - point 3 - Optimizing & Deployment Validation:	52	Fine tuning of the solutions to be done based on the criteria defined in Technical Specification of each solution and should assure a false positive rate not more than 10 % after 1 year for all solutions/services.	Please share the criteria/parameters that will be considered to assure false positive rate not more than 10% after 1 year for all solutions/services	The details shall be shared with the succesful bidder, after mutual discussion.

#	Section	Sub-section	Page	Clause / Requirement	Bidder Query	Response
69	Section E: Scope of Services	Training & Certification	54	Training & Certification	Kindly confirm the following - - no of participants for the training - Can the training be done online or it has to be done at onsite at LIC premises?	Please refer to the revised "Section E: Scope of Services"
70	2. Detailed Scope of Work	I. General Requirements	63	The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Our understanding is bidder has to leverage OEM PS services to do the end to end implementation. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
71	2. Detailed Scope of Work	I. General Requirements	63	The bidder should consider the detailed technical specifications as stated in the Annexure E while proposing for the solution. Bidder needs to provide complete end to end solution including applicable appliances, software, necessary accessories, active and passive components for efficient functioning of the proposed solution.	Our understanding is LIC will provide the underlying infra, hypervisor, OS and db, passive components . Kindly confirm	Please be guided by the RFP
72	2. Detailed Scope of Work	I. General Requirements	63	ii. Integration of each solution with other in scope solutions and other Network and Security solutions currently deployed in the environment as decided by the LIC.	Kindly share the details and the use cases for integration of existing network and security solutions (model no, OEM, technology) deployed for integration with the proposed solution	Please be guided by the RFP
73	2. Detailed Scope of Work	I. General Requirements	63	All the solutions should be seamlessly integrated with the LIC"s NTP solution and must be compatible with any provided NTP version	Please confirm which NTP solution is currently used by LIC	The details shall be shared with the successful bidder
74	2. Detailed Scope of Work	I. General Requirements	64	The bidder is required to undertake the migration of historical logs spanning a one-year duration from all existing solutions to new setup. This action is intended to enhance the security posture and to comply with the audit requirements	Our understanding is the solutions required as part of the RFP are new solutions and there are no existing solution and hence there is no migration that needs to be done. Please confirm	Only the logs of WAF are to be migrated .
75	2. Detailed Scope of Work	III. Network Access Control (NAC)	65	The vendor must provide the solution that must be compatible with our network infrastructure, supporting integration with our existing switches, routers, and firewalls	Please share the OEM, model and version details of switches, routers and firewall used at LIC	The details shall be shared with the successful bidder
76	5. Resource Deployment	SUPPORT PROCESS REQUIREMENT:	85	The Vendor has to construct a portal application with authentication to implement, assess and track various Trouble-tickets as well as to post important reports in the web-sites for higher official of LIC. The site has to be updated regularly by the on-site Personnel	Our undertsanding is bidder needs to propose a ITSM tool. If yes, please share the sizing details, technical specifications and sow for the same	Please refer to the revised "Section E: Scope of Services"
77	6. Project Timelines	b. NAC	87	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks= D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
78	6. Project Timelines	c. SSL Off loader	88	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks= D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
79	6. Project Timelines	d. WAF	88	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks= D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
80	6. Project Timelines	e. Mobile Device Management	88	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks= D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
81	6. Project Timelines	f. API Gateway, Management and Security	89	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks= D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	API Gateway and Security Solution has been removed from the scope of this RFP
82	6. Project Timelines	g. Virtual Desktop Interface (VDI)	89	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks= D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
83	Key Performance Indicators (KPI):	Parameter: Data Retention Period	94	Definition: The duration logs and data are retained within the CASB / NAC / WAF / SSL off loader/MDM/VDI/API Gateway, Management and Security before rotation or archiving. Target Service Level: 3 months, 1 year retention	Our understanding is LIC will provide the storage and archival for log retention. Kindly confirm	Please be guided by the RFP
84	Key Performance Indicators (KPI):	Parameter: Backup Frequency	94	Definition: How often data should be backed up to ensure recoverability. Target Service Level: Daily Incremental and Weekly Full Backup	Our understanding is LIC will provide the backup solution to ensure recoverability. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
85	Annexure F	point 2		CASB solution should support minimum of 25 users from day 1 with 5 year subscription/license/support and should have flexibility to scale as per future requirements with additional software/subscription license	Page 70 section 3 sizing requirements mentions 1000 roaming users whereas this point mentions 25 users from day 1. Kindly clarify what is the exact count to be considered for sizing and licensing	Please refer to the revised "Annexure F"
86	Annexure C: Eligibility Criteria	point 7	112	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request you to amend the clause as below - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to **at least 01 (one)** organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
87	Annexure C: Eligibility Criteria	point 8	113	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request you to amend the clause as below - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to **at least 01 (one) organisations** in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"

88	Annexure C: Eligibility Criteria	point 9	113	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Considering this is a new technology that is being adopted by organizations and some of the private firms may not have more than 500 branches. Hence request you to amend the clause as below - The bidder during the **last 7 years** preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to **at least 01 (one)** organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
89	Annexure D: Technical Scoring	point 2	115	The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. ⬛ Greater than 7 Years -> 10 Marks ⬛ Greater than 5 Years up to 7 Years -> 7 Marks ⬛ Greater than 3 Years up to 5 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The bidder should have relevant implementation and operational experience for **3 out of 7 in scope tools** scope tools to PSU/Government/Private/BFSI Sector Firms across different locations in India. ⬛ Greater than 7 Years -> 10 Marks ⬛ Greater than 5 Years up to 7 Years -> 7 Marks ⬛ Greater than 3 Years up to 5 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
90	Annexure D: Technical Scoring	point 3	115	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬛ 2 references of 65000 IP Addresses and above -> 10 Marks ⬛ 2 references of 50000 IP Addresses and above -> 7 Marks ⬛ 2 references of 25000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The Bidder during the **last 7 years** preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬛ 2 references of **60000** IP Addresses and above -> 10 Marks ⬛ 2 references of 50000 IP Addresses and above -> 7 Marks ⬛ 2 references of 25000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
91	Annexure D: Technical Scoring	point 4	115	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬛ 3 references and above -> 10 Marks ⬛ 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The Bidder during the **last 7 years** preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬛ 3 references and above -> 10 Marks ⬛ 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
92	Annexure D: Technical Scoring	point 5	115	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬛ 3 references and above -> 10 Marks ⬛ 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The Bidder during the **last 7 years** preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬛ **2 references and above** -> 10 Marks ⬛ **1 references** -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
93	Annexure D: Technical Scoring	point 6	116	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬛ 2 references of 10000 users and above -> 10 Marks ⬛ 2 references of 5000 users and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬛ **1 reference of 5000 users and above -> 10 Marks** ⬛ **1 reference of less than 5000 users -> 5 Marks** (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
94	Annexure D: Technical Scoring	point 7	116	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⬛ 4 references -> 10 Marks ⬛ 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The **bidder/OEM** must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⬛ 4 references -> 10 Marks ⬛ 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
95	Annexure D: Technical Scoring	point 8	116	The bidder must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⬛ 4 references -> 5 Marks ⬛ 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The **bidder/OEM** must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⬛ 4 references -> 5 Marks ⬛ 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"

96	Annexure D: Technical Scoring	point 9	116	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⯈ 4 references -> 5 Marks ⯈ 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The **bidder/OEM** must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⯈ 4 references -> 5 Marks ⯈ 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
97	Annexure D: Technical Scoring	point 10	116	The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP /CISA / CISM / OEM Level Certification. Every Additional 5 Resources -> 2 Marks subject to maximum of 10 marks 15 Resources -> 5 Marks (Supporting Document: Undertaking on bidder letter head needs to submit along with certification details and relevant evidence)	Request you to amend the clause as below - The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP /CISA / CISM / OEM Level Certification. **Every Additional 3 Resources** -> 2 Marks subject to maximum of 10 marks **10 Resources** -> 5 Marks (Supporting Document: Undertaking on bidder letter head needs to submit along with certification details and relevant evidence)	Please refer to the revised "Annexure D"
98	Annexure F - Technical Compliance	NAC Technical Specification	74	The Proposed Solution must support agent based and Agent less based approach	The NAC solution should support agentbased and agentless mode to achieve all feature & functionality which includes device visibility , Authentication, classification , Posture accessment , Remediations , Control and Automation, Does our understanding is correct?	Please be guided by the RFP
99	Annexure H: Manufacturer's Authorization Form (MAF)		121	_____ (OEM) certify that, the equipments being sold would not be declared End of Support (EoS) in the next 6Years and that _____ (OEM) shall supply suitable substitute in case EoS of equipments. Also _____ (OEM) certifies that the products being sold would be covered under Warranty / Support and support will be available for next six years (five years initially and one year if extension is provided) from the date of installation at LIC of India.	Requesting LIC to change the no of years from 6 years to 5 years only for EOS and also from Support point of view. Most of the securty solution "appliance" life is not more than 5 years. Hence request you to limit the years to 5 only.	Please refer to the revised "Annexure H"
100	Section C	Anexxure R	19		Quantity of WAF gateways and Management systems are not mentioned in Annexure R Bill of Quantity	Please refer to the revised "Section E: Scope of Services" and revised "Annexure G"
101	Annexure F - Technical Compliance	API GW	13	The solution should provide features to Convert between different data formats (e.g., JSON to XML).	We request LIC to reconsider older protocol supports like XML is an outdated API protocol, also JSON to XML translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The solution should should provide seamless integration with additional package to Convert between different data formats (e.g., JSON to XML) without adding overheads API-GW solution."	API Gateway and Security Solution has been removed from the scope of this RFP
102	Annexure F - Technical Compliance	API GW	19	The proposed solution should facilitate seamless SOAP to REST transformation, enabling interoperability by translating SOAP-based requests into RESTful API calls, promoting modern integration practices.	We request LIC to reconsider older protocol supports like SOAP is XML based outdated API protocol, also SOAP (XML) to REST (JSON) translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The proposed solution should seamless integration with additional package to translate SOAP to REST, enabling interoperability by translating SOAP-based requests into RESTful API calls as and when required without adding overheads API-GW solution, promoting modern integration practices".	API Gateway and Security Solution has been removed from the scope of this RFP
103	Annexure F - Technical Compliance	API GW	20	The solution should be designed to facilitate a developer organization by providing comprehensive tools, documentation, and support for efficient development.	We request LIC to consider that the mentioned features are getting fulfilled with development tools, not by API gateway, introducing it on API GW will increase overhead and it force developer to restrict themselves to limited features available on such tool. We request LIC to change this clause as: "The solution should be designed to facilitate to integrate it with developer organization by providing compatibility with multiple tools and support for efficient development with the Security of authentication, authorization, payload sanitization and WAF signature inspection"	API Gateway and Security Solution has been removed from the scope of this RFP
104	Annexure F - Technical Compliance	API GW	31	The API gateway should implement streaming APIs using compatible protocols like WebSocket, WebSub, or server-sent events.	We request LIC to kindly change this clause as webSub is a protocol usually used to push content by many websites, including all blogs served by Blogger and WordPress.com news sites. This use case seems to be irrelevant to LIC. Recommended revised clause: "The API gateway should implement streaming APIs using compatible protocols like WebSocket and server-sent events and support WebSub via plugins/packages."	API Gateway and Security Solution has been removed from the scope of this RFP
105	-	-	Additional query	Kindly confirm the total number of applications to be considered for onboarded on SSLO during the deployment phase.	-	Please be guided by the RFP
106	Annexure F - Technical Compliance	NAC Technical Specification > Point no. 13	Excel sheet-1	LIC has a heterogeneous network environment comprising of network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of any hardware and software	Please let us know that all the network devices in LIC environment are supporting IEEE RADIUS authentication, RADIUS CoA, downloadable ACL, Dynamic ACL and Dynamic VLAN assignment, Multi-Session authentication and multi-domain authentication for policy enforcement on the network device.	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .
107	Annexure F - Technical Compliance	NAC Technical Specification > Point no. 14	Excel sheet-1	The Solution should be compatible with the existing network environment of the LIC and any future procurement	Please let us know that all the existing network environment in LIC are supporting IEEE RADIUS authentication, RADIUS CoA, downloadable ACL, Dynamic ACL and Dynamic VLAN assignment, Multi-Session authentication and multi-domain authentication for policy enforcement on the network device.. Same protocol should be supported in future procurement network device as well.	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .
108	Annexure F - Technical Compliance	NAC Technical Specification > Point no. 46	Excel sheet-1	The proposed solution should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma.	Request is to change this clause to The proposed solution should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma or should support importing of endpoints using XML/API. If Device details information is stored as an XML file, which can be password protected. administrator will enter the same secret key to import the device into the NAC server.	Please refer to the revised "Annexure F"

#	Section	Subsection	Ref	Clause	Query	Response
109	Annexure F - Technical Compliance	NAC Technical Specification > Point no. 69	Excel sheet-1	The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001, etc.) and any applicable laws and regulations (such as IRDAI, DPDP Act etc.)	Please let us know that GDPR compliance or NDPP certification is also applicable for this compliance clause.	Please refer to the revised "Annexure F"
110	2. Detailed Scope of Work	I. General Requirements	63	The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period. Over the 5-year contract period, bidder may consider an increase of 50% in the number of devices or solutions to be monitored when determining system specifications.	In the sizing requirements for NAC , its advised to refer Tech Specs , point 67 towhich mentions "Total of 127000 endpoint devices and scalable to 160000 devices" above is only 26% and doesnt align with this clause. with 50% increase the scalability ask has to be 191000 , Request this be clarified so the ambiguity doesnt hold	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
111	2. Detailed Scope of Work	I. General Requirements	63	The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Request this be modified as below The bidder / System Integrator shall engage the services of respective OEMs / OEM certified Partner for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Please refer to the revised "Section E: Scope of Services"
112	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall ensure that the OEM(s) has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC"s infrastructure during the tenure of this project.	Request this be modified as below The bidder shall ensure that the OEM(s)/ OEM certified Partener has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC"s infrastructure during the tenure of this project.	Please refer to the revised "Section E: Scope of Services"
113	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder"s resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Request this be modified as below The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM / OEM certified Partner as decided by LIC at the time of implementation. The bidder"s resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM / OEMs certified Partner.	Please refer to the revised "Section E: Scope of Services"
114	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall also engage the services of the respective OEMs for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Request this be modified as below The bidder shall also engage the services of the respective OEMs / OEMs Certified Partner for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Please be guided by the RFP
115	2. Detailed Scope of Work	I. General Requirements	63	The bidder and OEM services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Request this be modified as below The bidder and OEM / OEMs certified Partner services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Please refer to the revised "Section E: Scope of Services"
116	2. Detailed Scope of Work	I. General Requirements	63	The bidder and OEM services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Request this be modified as below The bidder and OEM/OEM certified Partner services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Please refer to the revised "Section E: Scope of Services"
117	2. Detailed Scope of Work	I. General Requirements	64	The vendor should arrange for a comprehensive deployment audit done by OEM after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation.	Request this be changed as The vendor should arrange for a comprehensive deployment audit done by OEM / OEMs certified partner after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation.	Please be guided by the RFP
118	2. Detailed Scope of Work	I. General Requirements	64	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	In the sizing requirements for NAC , its advised to refer Tech Specs , point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices" With 20% YoY growth , the scalability ask should be 263000 , Request this be clarified so the ambiguity doesnt hold and also we inclued the right breakdown of charges for the additional licenses as ked in this clause	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
119	6. Project Timelines	b. NAC	87	2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. -= T + 5 Weeks= D	Request this be changed to below 2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. -= T + 10 Weeks= D	Please refer to the revised "Section E: Scope of Services"
120	Annexure F: Technical Compliance	NAC #67	119	67. The Proposed solution should provide comprehensive visiblity of the network by automatically discovering , classifying and enforcing policy for endpoints connected to the network and must have capacity to support the appropriate service for a total of 127000 endpoint devices and scalable to 160000 devices	Request the count of end user devices and the headless devices be please shared out of the asked 127000 now and 160000 devices in future	The details shall be shared with the successful bidder
121	Annexure F: Technical Compliance	NAC #69	119	69. The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001 etc) and any applicable Laws and regulations (such as IRDAI, DPDP Act etc)	while we are ISO27001 complied , DPDP act is not fully mature and may take some time to freeze, we request LIC to remove this and also share the IRDAI Laws and regulations Document to check for compliance	Please refer to the revised "Annexure F"
122	Annexure F: Technical Compliance	NAC #13	119	13. LIC has a hetrogenious network environment comparising network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of any hardware and software	The Network devices should support IEEE 802.1x and Radius COA standards to support NAC.Request if the Netwook devices Make and model be shared , we can thoroughly check and approprriately respond.	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .
123	Annexure F: Technical Compliance	NAC #14	119	The Solution should be compatilbe with the existing network environment of the LIC and any future procurement	while existing network environt is addressed in #13 of the tech specs , we request LIC to procure any routers/switches in future to have support for IEEE 802.1x and Radius COA standards	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .
124	Annexure F: Technical Compliance	NAC #14	119	75 The proposed NAC solution must be in the leaders quadrant in the Gartners magic quadrant for Network Access control in the last published report. This clause will not be applicable for OEMs qualifying under make in India category	Gartner stopped publishing these reports for NAC off late as this solution is matured well , we see the last report as 2019 , request LIC to confirm if the report from 2019 will hold well or let us know if alternate consulting body reports may be considered	Please be guided by the RFP

125	Annexure H: Manufacturer's Authorization Form (MAF)	N/A	121	_ (OEM) certify that, the equipments being sold would not be **declared** End of Support (EoS) in the next 6Years	Request this be rephrased as below since the declaration of End of support and actual EOS of the product is 2 different interpretations _ (OEM) certify that, the equipments being sold would not be End of Support (EoS) in the next 6Years	Please refer to the revised "Annexure H"
126	Compliance			The CASB Solution must have HTTP/2 support from day 1.	This is Web Security (SWG) feature. It is requested to remove this clause.	Please refer to the revised "Annexure F"
127	Compliance			The CASB Solution must have 99% uptime SLA	Considering business applications access via Cloud Service provider,SLA's for Cloud Vendor has to high. Our request to consider 99.999% uptime SLA instead of 99%	Please refer to the revised "Annexure F"
128	Compliance			The solution must have Web IPS (Signatures) to protect against targeted user-agent threats	This is SWG feature and not CASB feature. CASB is meant to protect SaaS applications and not vulnerabilities.This need SWG license consideration. Kindly relax the point.	Please refer to the revised "Annexure F"
129	22. Patent Rights and other litigation costs:		34	In no event shall LIC be liable for any indirect, incidental or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered. For this purpose, it would be immaterial how such liability may arise, provided that the claims against customers, users and service providers of LIC are considered as a direct claim	We propose to make this clause mutual.	Please be guided by the RFP
130	33. Limitation of Liability		37	Except in cases of criminal negligence or wilful misconduct, and in the case of infringement pursuant to Conditions of Contract Clause, the vendor shall not be liable to LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC; and the aggregate liability of the bidder to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.	Please clarify infringement in what context. Conditions of Contract Clause in a capitalised term which is not defined in the RFP. Hence it is not possible to have a clear interpretation of this clause. Please confirm what all is proposed to be kept out of Limit of Liability cap and for what is the Bidder supposed to bear Indirect Liability. Also repair and replacement of equipment terms will be as per the terms provided by the OEM. NTT does not manufacture any equipment.	Please be guided by the RFP
131	36. Indemnifying LIC	A.	38	Against all actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC. Against all demands or responsibilities arising from accidents or loss of life as a result of vendor's negligence.	Slight Modification Requested:- Against all actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC **as a result of breach of the terms and conditions of the RFP by the Vendor**. Against all demands or responsibilities arising from accidents or loss of life as a result of vendor's **gross** negligence.	Please be guided by the RFP
132	46. Award and Signing of Bid Contract	d)	42	Within 14 working days of receipt of the Contract Form, the successful vendor shall sign and date the Contract and return it to LIC.	If there are any additional terms other than the ones mentioned in the RFP, it will be subject to review and acceptance by the Vendor.	Please be guided by the RFP
133	7. Intellectual Property Rights		99	Entire clause on Intellectual Property Rights	For NTTI services, these services are non-exclusive and hence there shall be no transfer of IPRs. For OEM/ OSD products/ services transfer of IPRs shall be as per the terms offered by the OEM/ OSD. Warranties on IPRs on equipment shall be as per the terms provided by the OEM. There should not be any warranties on IPRs for services.	Please be guided by the RFP
134	3. Activity Schedule	Earnest Money Deposit	11	EMD to be submitted of Rs. 2 Crores	Rs. 2 Crores is a very high value of EMD. Kindly request LIC to keep EMD in range of 2% of estimated budget of RFP.	Please be guided by the RFP
135	Commercial Bid Format				The total value (Column M) does not multiply the price with quantity provided. Kindly request LIC to rectify the commercial format and re-share.	Please refer to the revised "Annexure G"
136	9. Pricing, Billing, Duties and Taxes		24	c) Prices once fixed will be valid throughout the entire contract period. The Vendor should not, under any circumstances, request for an increase in the prices once prices are approved by LIC. No price variation relating to increases in Government levies/ taxes/ cess/ customs duty & excise duty including any newly introduced taxes shall be permitted.	Taxes, Duties (including Custom Duty), Levies etc are not within bidder's control. Hence the bidder requests LIC to allow for price revision to the extent of revision in any of these factors by Honourable Government.	Please refer to the revised "Pricing, Billing, Duties and Taxes" and revised "Period of Validity of Bids"
137	12. Evaluation process for selection of bidder		28	p) Computation Methodology for rating bidders on 'Technical plus Commercial basis': q) There would be a weightage of 70% to the technical score and 30% for the final Commercial price quoted by the bidder at the end of online reverse auction. r) It would be normalized as under for each bidder: - Total Score (up to 3 decimals) = {(T x 0.7) / Thigh} + {(LLow x 0.3) / L}	Since LIC is evaluating the bids on basis of Technical & Commercial with 70:30 weightage, then kindly request LIC to request for a final price submission alongwith technical proposal to shorten the timeline for evaluation. This similar evaluation methodology is used by RBI & SEBI in their bids.	Please be guided by the RFP
138	25. Placing of Orders and Making Payments		35	a) The Central Office of LIC at Mumbai will place orders (either in full or in phases) with successful bidder for deliverables under this RFP at any time during the validity period of this tender. b) LIC reserves the right to place repeat orders for additional services/ reassessment on the same terms & conditions during the validity of the contract.	The prices are dependant on Taxes, Duties (including Custom Duty), Levies, OEM List Prices, OEM Discounting, USD-INR exchange rate etc. These factors are not within bidder's control and hence we request LIC to allow for price revision on mutually agreeable basis for any subsequent additional order after the 1st PO.	Please refer to the revised "Pricing, Billing, Duties and Taxes" and revised "Period of Validity of Bids"
139	55. Varying the Services	I. Variations proposed by LIC	46	I. Variations proposed by LIC – LIC reserves the right to initiate any change in the scope of contract. Vendors must factor in a maximum of 25% scope changes within the services, appliances, licenses, etc. cost to be quoted in the commercial bid. Any change in the scope beyond this 25% will be informed to the vendor in writing.	25% is a very high percentage for scope change to be factored for Services, Appliances and Licenses. Kindly request LIC to provide Change Requests for additional requirement so that the bidder can provide a best possible price during evaluation.	Please be guided by the RFP
140	7. Service Level Agreements (SLAs) & Penalties		90	Penalty due to delay of 0.2% of total PO value per day.	0.2% of penalty per day is very high value. Kindly request LIC to levy penalty of 0.2% of penalty per week of the undelivered value of materials.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
141	7. Service Level Agreements (SLAs) & Penalties	Penalty Caps	96	The total penalty for onsite support shall not exceed 100% of the quarterly charges payable for onsite support for reasons other than absence.	Kindly request LIC to cap the penalty at 10% of quarterly payable for onsite support.	Please be guided by the RFP

#	Section	Sub	Page	RFP Clause	Query / Request	Response
142	Section G: Payment Terms & Condition		104	The payment terms defined in RFP are as below: o Delivery – 30% o Installation & Integration – 40% o After Go-Live – 25% o Training – 5%	Kindly request LIC to revise the payment terms as below as per industry standards: o Delivery – 70% o Installation & Integration – 20% o After Go-Live – 5% o Training – 5%	Please refer to the revised "Payment Terms & Conditions"
143	Section H	Annexure C- Eligibility Criteria #3	112	The bidder should be in operating-profit (EBITDA i.e., Earnings before Interest, Tax, Depreciation & Amortization) during the last 03 (three) years preceding the date of this RFP or The bidder should have made profit (before tax) in any of the 03 (three) out of last 05 (five) financial years preceding the date of this RFP and should be having positive net worth for the last 03 (three) financial years preceding to the date of this RFP.	Considering Bidder's capability to manage the long term sustainability and financial health and manage the Critical network deployment we request LIC to modify clause as below : Bider should have made profit (before tax) in **all the last three** financial years preceding the date of this RFP and should be having positive networth for the last 03 (three) financial years preceding to the date of this RFP.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
144	Section H	Annexure C- Eligibility Criteria #9	112	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02(two organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	CASB is a relatively newer technology solution.Request LIC to remove clause as below OR Please modify clause as The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the **Web Proxy/ Web Security Gateway/CASB** to at least02 (two)organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
145	Section H	Annexure D- Technical Criteria #2	115	The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. • Greater than 7 Years -> 10 Marks • Greater than 5 Years up to 7 Years -> 7 Marks • Greater than 3 Years up to 5 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request LIC to clarify if bidder experience for 3 0r 4 out of 7 inscope tools Is being evaluated in this criteria for technical scoring.	Please refer to the revised "Annexure D"
146	Section H	Annexure D- Technical Criteria #3	115	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: • 2 references of 65000 IP Addresses and above -> 10 Marks • 2 references of 50000 IP Addresses and above -> 7 Marks • 2 references of 25000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request LIC to modify clause as below : The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: • 2 references of 55000 IP Addresses and above -> 10 Marks • 2 references of 40000 IP Addresses and above -> 7 Marks • 2 references of 25000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
147	Section H	Annexure D- Technical Criteria #6	116	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: • 2 references of 10000 users and above -> 10 Marks • 2 references of 5000 users and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to modify clause as below: The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: 1 reference of 20000 users and above-->10 Marks • 2 references of 10000 users and above -> 5 Marks • 2 references of 5000 users and above -> 3 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
148	Section H	Annexure D- Technical Criteria #7	116	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India • 3 references -> 10 Marks • 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 50 APIs in the PSU/Government/Private/BFSI Sector Firms. • 2 references and above -> 10 Marks • 1 reference -> 5 Marks Atleast one reference should support 1000 Transactions per second. (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
149	Section H	Annexure D- Technical Criteria #8	116	The bidder must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India • 3 references -> 5 Marks • 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	CASB is a relatively newer technology solution.Request LIC to remove clause as below OR Please modify clause as The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the **Web Proxy/ Web Security Gateway/CASB** to at least02 (two)organisations in PSU/Government/Private/BFSI Sector Firms • 2 or More references -> 5 Marks • 1 references -> 2 Marks	Please refer to the revised "Annexure D"

150	Section H	Annexure D-Technical Criteria #9	115	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India •☐ references -> 5 Marks •☐ references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India •☐ references and above -> 10 Marks •☐ reference -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
151	7	Implementation SLA	90	Delay in Submission of HLD and LLD beyond 6 weeks from Date of Issue of Purchase order	Request to modify clause: Delay in Submission of HLD and LLD beyond 8 weeks from Date of Issue of Purchase order	Please refer to the revised Service Level Agreements (SLAs) & Penalties
152	7	Implementation SLA	90	Penalty is on total deal value	Request to consider penalty as % of delayed deliverable	Please refer to the revised Service Level Agreements (SLAs) & Penalties
153	7	Implementation SLA	93	Parameter : Uptime - penalty of 0.25% of total PO value per week of delay or part of thereof	Request to consider penalty as a % of 0.25% of quarterly support value	Please refer to the revised Service Level Agreements (SLAs) & Penalties
154	7	Implementation SLA	93 to 96	Penalty is on total deal value	Request Penalty to be aligned to be quarterly invoice value	Please refer to the revised Service Level Agreements (SLAs) & Penalties
155	7	Implementation SLA	96	The total penalty for delivery & installation shall not exceed 10% of the PO value	Request penalty to be capped to total value of delayed deliverable.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
156	7	Implementation SLA	96	The total penalty for onsite support shall not exceed 100% total quarterly charges	Request penalty to be changed to " The total penalty should not exceed 10% of quarterly invoice value.	Please be guided by the RFP
157	Section E	Scope of Work	69	The proposed API Gateway, Management and Security solution should provide real time analytical insights and data.	The Solution can provide user login and session statistics and this can be published to any advanced SIEM for further analysis. Request LIC to confirm this understanding on insights and data.	API Gateway and Security Solution has been removed from the scope of this RFP
158	Annexure F	Annexure F API Technical Specifications	The solution should achieve and maintain compliance with industry standards, such as PCI DSS, and provide detailed reporting for audit purposes.	AWe understand compliance and encryption to PCI -DSS standards will also be undertaken at the API Creation Activity/End point stage.	API Gateway and Security Solution has been removed from the scope of this RFP
159	Annexure F	Annexure F API Technical Specifications	The solution should provide automated discovery of backend services and APIs.	We understand this is a feature of WAF solution, hence kindly remove this compliance parameter under API Technical Specifications	API Gateway and Security Solution has been removed from the scope of this RFP
160	Section E	Scope of Work	64	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	Request LIC to clarify the Scalability over 5 Year period .	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
161	Section E	Service Level Uptime	92	f the LIC"s firewall system uptime for any of the three locations is below 99.9% calculated on monthly basis.	Request LIC to clarify the uptime mention of the "Firewall System" here.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
162	Resource Deployment		72	Additional Point Suggested	To maintain operational efficiencies during the contract term and to ensure minimum level of resource quality request LIC to include the following floor limit of resource cost . L1 Resource/Security Analyst - 8 Lacs Per annum L2 Resource/ Security Analyts - 10 Lacs per annum L3 Resource/ Solution Analyst- 15 Lacs per annum PM - 20 Lacs Per annum	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
163	Section H	Annexure F, 86	The solution must protect system against WASC Wec Security Attack classification.	Request to modify the clasue as "The solution must protect system against WASC Wec Security Attack classification or OWASP top 10."	Please refer to the revised "Annexure F"
164		Annexure F Additional point (must have)	The SSLO devices should be STIP compliant.	STIP compliance is part of Common Criteria (CC) that provides a common set of requirements for the security functionality of IT products and the assurance measures to be applied to the IT products during a security evaluation. Does LIC require the SSLO device to be STIP compliant?	Please be guided by the RFP
165	-	Annexure F Additional query	Kindly confirm the total number of applications to be considered for onboarded on SSLO during the deployment phase.	-	Please be guided by the RFP
166	2. Detailed Scope of Work	VII. API Gateway, Management and Security	68	VII	What are the backend systems with which the API Gateway needs to integrte with? Are there backend systems with published APIs available today within LIC? Can you give a list of systems to be integrated with?	API Gateway and Security Solution has been removed from the scope of this RFP
167	2. Detailed Scope of Work	VII. API Gateway, Management and Security	68	VII	Who are the External/Internal users or consumers of the APIs and the API Gateway?	API Gateway and Security Solution has been removed from the scope of this RFP
168	2. Detailed Scope of Work	VII. API Gateway, Management and Security	68	VII	How are the APIs being accessed today?	API Gateway and Security Solution has been removed from the scope of this RFP
169	2. Detailed Scope of Work	VII. API Gateway, Management and Security	68	VII	Are there plans to monetize APIs? If so, are there any business plans?	API Gateway and Security Solution has been removed from the scope of this RFP
170	2. Detailed Scope of Work	VII. API Gateway, Management and Security	68	VII	Is there a requirement for an internal/external facing Developer Portal for APIs?	API Gateway and Security Solution has been removed from the scope of this RFP

171	2. Detailed Scope of Work	VII. API Gateway, Management and Security	68	VII	What is the average size of the payload of APIs, in KBs?	API Gateway and Security Solution has been removed from the scope of this RFP
172	2. Detailed Scope of Work	VII. API Gateway, Management and Security	68	VII	What is the TPS (no. of API calls of an average payload) performance required for the API Gateway?	API Gateway and Security Solution has been removed from the scope of this RFP
173	2. Detailed Scope of Work	VII. API Gateway, Management and Security	68	VII	What is the average response time required for the API GW?	API Gateway and Security Solution has been removed from the scope of this RFP
174	7. SLAs and Penalties	KPI	95	11	Custom connectors, if required: This clause requires modification. There is no detailed list of backend systems to identify whether custom connectors are required or not. Without that, it is not possible to decide whether custom connectors or required or not.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
175	7. SLAs and Penalties	KPI	95	12	Device integration with CASB / NAC / WAF / SSL off loader / MDM / VDI / API Gateway, Management and Security. What new IT systems, applications are expected in LIC? If any of the new systems or applications in LIC are to be integrated in future with the above list of solutions, then those new systems or applications should follow the protocols and communication mechanisms that these solutions follow and not the other way around.	Please be guided by the RFP
176	Annexure F - Technical Compliance	NAC Technical Specification > Point no. 69	Excel sheet-1	The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001, etc.) and any applicable laws and regulations (such as IRDAI, DPDP Act etc.)	Please let us know that GDPR compliance or NDPP certification is also applicable for this compliance clause.	Please refer to the revised "Annexure F"
177	Section C	Clause 24	34	b)The PBG should be valid for a period to cover the expected contract period of 60 months and additional 3 months after the date of expiry of the contract from the date of its submission to LIC.	Bidder request to allow rolling BG for 12 months period of 10% of contract value. The BG will be renewed every year till the end of contract period and additional 3 months	Please be guided by the RFP
178	Section C	Clause 27	35	a)Bids shall remain valid for 12 months from the last date of bid submission as prescribed by LIC, in the Activity Schedule. LIC shall reject a bid as non-responsive if the bid is submitted with a shorter validity period	Bidder request to reduce bid validity to 90 days only.	Please be guided by the RFP
179	Section G	Clause 1	104	Payment Terms & Conditions	Bidder request to change the milestone as below 1. 70% on delivery of SW 2. 20% on installation and integration 3. 5% on FAT 4. 5% on completion of training	Please refer to the revised "Payment Terms & Conditions"
180	Pre-Integrity Pact		5	Sanctions for Violations	We request that this be restricted to wilful actions and with the bidder's knowledge.	Please be guided by the RFP
181	7		17	Responding to this RFP and submission of the bid by the Bidder will be deemed as consent from the Bidder to all the terms and conditions mentioned in this RFP along with its Annexure, clarifications, appendices, addenda, corrigenda issued. The terms and conditions for the bidders who participate in this RFP are specified in the Section named "Terms and Conditions". Responding to this RFP and submission of the bid by the Bidder will be deemed as consent from the Bidder to all the terms and conditions mentioned in this RFP document and the contents of the RFP along with the Annexure(s), clarifications/modifications issued, if any, will be contractually binding on the bidders. All these terms and conditions and the contents of the RFP along with the Annexure(s), clarifications/modifications issued will form the part of the purchase orders/any resulting contracts, to be issued to the successful bidder/s from time to time as an outcome of this RFP Process.	It is submitted that certain terms of the RFP need modification and all such terms may not be discussed during the pre-bid stage. It is hence requested to permit bidders to submit their revisions, suggestions, additions etc. to the terms of the RFP as part of the bid submission. We would kindly request the following edits to be made to the clause: "Responding to this RFP and submission of the bid by the Bidder will be deemed as consent from the Bidder to all the terms and conditions mentioned in this RFP document and the contents of the RFP along with the Annexure(s), clarifications/modifications issued, if any, will be contractually binding on the bidders. Subject to mutual agreement between the parties, Aall these terms and conditions and the contents of the RFP along with the Annexure(s), clarifications/modifications issued will form the part of the purchase orders/any resulting contracts, to be issued to the successful bidder/s from time to time as an outcome of this RFP Process." We would also request similarly worded language to be amended along the same lines - such as under clause 9 and annexure A.	Please be guided by the RFP
182	15	b	30	Violation of NDA may lead to legal action and blacklisting.	We cannot agree to blacklisting for breach of NDA. Please accept the below modification: "Violation of NDA may lead to legal action and blacklisting ." We can only agree to this for matters relating to fraud and corrupt practices. We request for the same amendment to be made for clause 21(1)(b) on page 32.	Please be guided by the RFP
183	19	g	31	LIC may cancel any procurement under this RFP at any time without assigning any reasons whatsoever. The decision of LIC will be final in this matter.	We would kindly request that the clause be clarified for the following questions: a. can the procurement be cancelled at any point? - e.g after the order has been placed and the vendor has initiated progress on that front b. would all payments for procurements till such date be made? c. would there be a minimum number of days notice required for such cancellation for convenience?	Please be guided by the RFP
184	22		33	In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, or industrial design rights arising from the use of the systems or any parts thereof with relation to the Hardware deliverables, in LIC's country, the Bidder will act expeditiously to extinguish such claim.	We would kindly request that this be amended in a manner that would reflect that we be liable for permitted uses of the IPR, such as below: "In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, or industrial design rights arising from the permitted and agreed upon use of the systems or any parts thereof with relation to the Hardware deliverables, in LIC's country, the Bidder will act expeditiously to extinguish such claim."	

185	22		34	In no event shall LIC be liable for any indirect, incidental, or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered	We would request that this clause be made mutual to reflect as below: "In no event shall ~~LIC~~ **either party** be liable for any indirect, incidental, or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered."	Please be guided by the RFP
186	24	b	34	The PBG should be valid for a period to cover the expected contract period of 60 months and additional 3 months after the date of expiry of the contract from the date of its submission to LIC.	We request that the PBG period be the same as the contract period, i.e. of 60 months.	Please be guided by the RFP
187	24	g	34	The PBG may be invoked for entire amount if the vendor backs-out of his obligations as per this tender or if the fresh PBG is not received by LIC one month prior to the expiry of the earlier PBG; apart from other actions that may be decided by LIC.	We request that the clause be deleted and replaced as below: "Subject to a notice and cure period of not less than 30 days, the PBG may be invoked solely for material breaches of the Contract." PBG must be invoked only for material breaches and the bidder must be provided a cure period to rectify breaches before PBG is invoked.	The PBG may be invoked for entire amount, after providing a cure period of 30 days in writing, if the vendor backs-out of its obligations as per this tender or if the fresh PBG is not received by LIC one month prior to the expiry of the earlier PBG; apart from other actions that may be decided by LIC.
188	24	h	34	If vendor fails to submit the required PBG within 28 days period as mentioned above, penalty of Rs.5,000/- per day (subject to maximum penalty of Rs.1,00,000/-) will be imposed. In case the selected bidder fails to submit performance bank guarantee even after the elapse of 35 days from the date of letter issued for selection as the "selected vendor", LIC at its discretion, may cancel the allotment of the contract to the concerned bidder and may blacklist them.	We would request that the clause be amended as follows: " ~~If vendor fails to submit the required PBG within 28 days period as mentioned above, penalty of Rs.5,000/- per day (subject to maximum penalty of Rs.1,00,000/-) will be imposed.~~ In case the selected bidder fails to submit performance bank guarantee even after the elapse of 35 days from the date of letter issued for selection as the "selected vendor", LIC at its discretion, may cancel the allotment of the contract to the concerned bidder ~~and may blacklist them~~ ."	Please be guided by the RFP
189	24	j	35	The PBG will be invoked in full or part (to be decided by LIC) if the bidder fails to honour expected deliverables or part as per this RFP after issuance of PO during the period of contract. i. The bidder fails to honour expected deliverables or part as per this RFP after issuance of PO. ii. Any legal action is taken against the bidder restricting its operations. iii. Any action taken by statutory, legal or regulatory authorities for any breach or lapses which are directly attributable to the bidder iv. LIC incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.	We request that the clause be amended as below: "The PBG will be invoked in full or part (~~to be decided by LIC~~) **in the eventuality of a material breach** ~~if the bidder fails to honour expected deliverables or part as per this RFP after issuance of PO~~ during the period of contract **and the selected vendor will be provided notice and a cure period of not less than 30 days to rectify such material breaches.** ~~i. The bidder fails to honour expected deliverables or part as per this RFP after issuance of PO.~~ ~~ii. Any legal action is taken against the bidder restricting its operations.~~ ~~iii. Any action taken by statutory, legal or regulatory authorities for any breach or lapses which are directly attributable to the bidder~~ ~~iv. LIC incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.~~ We would kindly submit that the PBG must be invoked only for material breaches and the bidder must be provided a cure period to rectify breaches before PBG is invoked.	Please be guided by the RFP
190	27	a	35	Bids shall remain valid for 12 months from the last date of bid submission as prescribed by LIC, in the Activity Schedule.	We would kindly request that this duration be shortened to 3 months, as it becomes difficult to keep all the price rates for the same services fixed for a longer duration.	Please refer to the revised "Period of Validity of Bids"
191	27	f	36	The commercial offer shall be on a fixed price basis for the contact period. No upward revision in the price would be considered on account of subsequent increases during the offer validity period except for GST and any other applicable taxes.	We would request that this clause be deleted as it becomes difficult to account for all potential change in prices (both upward and downward) for the entire duration of 60 months, i.e. 5 years, owing to several factors out of our hands.	Please refer to the revised "Period of Validity of Bids"
192	33		37	Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Conditions of Contract Clause, the vendor shall not be liable to LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC; and the aggregate liability of the bidder to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.	We would request that the clause be amended accordingly: "Except in cases of criminal negligence or willful misconduct, ~~and in the case of infringement pursuant to Conditions of Contract Clause,~~ ~~the vendor~~ **neither party** shall ~~not~~ be liable to **the other** ~~LIC~~, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or **business**, interest costs, ~~provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC~~; and the aggregate liability of **both the parties** ~~the bidder to LIC~~, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder ~~provided that this limitation shall not apply to the cost of repairing or replacing defective equipment~~." We cannot agree to indirect and consequential damages for IPR infringement. The exclusion of indirect and consequential damages must also apply to LDs. Limitation of Liability must also apply to costs of repairs and replacements of defective equipment.	Please be guided by the RFP
193	34	a	37	The vendor shall be liable for any delay in execution or failure of their respective obligations under this agreement except for delay caused by occurrence of events beyond control of the vendor, including but not limited to natural calamities, fire, explosions, floods, power shortages, acts of God, hostility, acts of public enemy, wars, riots, strikes, sabotage, order/action, or regulations of government, local or other public authorities.	We would kindly request that this clause be edited as below: "The vendor shall be liable for any delay in execution or failure of their **previously agreed upon** respective obligations, **beyond the cure period granted**, under this agreement except for delay caused by occurrence of events beyond control of the vendor, including but not limited to natural calamities, fire, explosions, floods, power shortages, acts of God, hostility, acts of public enemy, wars, riots, strikes, sabotage, order/action, or regulations of government, local or other public authorities. **For clarity - such an event will not preclude LIC from its payment obligations to the vendor**." Please accept new insertion excusing performance in case of Force Majeure situation. LIC's payment obligations not to be covered under such excusing of performance.	Please be guided by the RFP
194	35	c	38	The Vendor shall not be entitled to suspend the Service(s) or the completion of the job, pending resolution of any dispute between the Parties and shall continue to render the Service(s) in accordance with the provisions of the RFP notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings.	We cannot agree to not having a right to suspend the works under the Contract if the nature of the dispute is such that it would be impractical for the works to be continued. Please accept the below modification. "c) **Unless the nature of the dispute is such that it would be impractical for the Service(s) to be continued, t** ~~T~~ he Vendor shall not be entitled to suspend the Service(s) or the completion of the job, pending resolution of any dispute between the Parties and shall continue to render the Service(s) in accordance with the provisions of the RFP notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings."	Please be guided by the RFP

#	Col1	Col2	Col3	Clause	Request	Response
195	35	d	38	The work under contract shall continue during the Arbitration proceedings and no payment due or payable to the Contractor shall be withheld on account of such proceedings.	We request the clause be amended as below: "The work under contract shall continue during the Arbitration proceedings and no payment due or payable to the **bidder or** Contractor shall be withheld on account of such proceedings."	Please be guided by the RFP
196	36	A.a	38	Against all actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC.	We request that the clause be amended as below to only include direct claims: "Against all **direct** actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC."	Please be guided by the RFP
197	42	f	41	Recover any dues payable by the selected Vendor from any amount outstanding to the credit of the selected Vendor, including the pending bills and/or invoking PBG or other payment pending from the vendor, if any, under this contract.	We request that the bidder also have a say in this and it is not a unilateral decision.	Please be guided by the RFP
198	47	e	43	LIC may, at any time, by a prior written notice of one week, terminate the successful bidder and / or reduce the scope of the Services	We would kindly request for this time frame to be 30 days as opposed to one week in order to be able to adjust the requirements accordingly.	Please be guided by the RFP
199	47	k	44	LIC may at any time terminate the Contract by giving written notice to the Successful bidder, if the Successful bidder becomes bankrupt or otherwise insolvent. In this event, the termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to LIC.	We would humbly submit that by going bankrupt or insolvent, it should not preclude us from receiving payments for services that we have already provided and have been accepted. We would request that the clause be amended as follows: "LIC may at any time terminate the Contract by giving written notice to the Successful bidder, if the Successful bidder becomes bankrupt or otherwise insolvent. ~~In this event, the termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to LIC.~~ "	Please be guided by the RFP
200			New Clause To Be Inserted	Either party may terminate this Agreement on written notice if the other fails to meet any material obligation and fails to remedy the breach within a 30 day period after being notified in writing of the details. If either party becomes insolvent, unable to pay debts when due, files for or is subject to bankruptcy or receivership or asset assignment, the other party may terminate this Agreement and cancel any unfulfilled obligations. Any terms in the Agreement which by their nature extend beyond termination or expiration of the Agreement will remain in effect until fulfilled and will apply to both parties' respective successors and permitted assigns.	New Clause To Be Inserted. Both parties must have a right to terminate.	Please be guided by the RFP
201	Section E	1	50	Please note, the below list of activities is only indicative and not an exhaustive list.	We would kindly request that the list be an exhaustive one so as to account for all the services and costs.	Please be guided by the RFP
202	Section E	1	53	The SI shall have to comply with LIC"s IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the finally selected Bidder.	We kindly request that this policy be shared with us beforehand so that we can ensure compliance with the same.	The details shall be shared with the successful bidder
203	2	II	64	The vendor must provide the solution that must be compliant with GDPR, DPDP, IRDAI.	We would humbly request that the specific sections be called out, particularly for compliance with IRDAI, as it can be difficult to ensure compliance with otherwise.	Please be guided by the RFP
204	Section F	1.d.i.	97	LIC may cancel the purchase order placed which will be conveyed to the vendor in writing.	We would kindly request that the clause be clarified for the following questions: a. can the procurement be cancelled at any point? - e.g after the order has been placed and the vendor has initiated progress on that front b. would there be a minimum number of days notice ?	Please be guided by the RFP
205	Section F	1.d.vi.	97	Termination of contract and blacklisting.	We would request that the clause be amended as follows, as we submit that blacklisting should be resorted to only for fraudulent or corrupt practices: "Termination of contract ~~and blacklisting~~ ."	Please be guided by the RFP
206	Section F	1.e	97	In case of cancellation of orders due to delay in deliveries/installations or deficiency in services etc., besides the penalty being charged, the vendor may also be blacklisted by Life Insurance Corporation of India & may not be allowed to participate in any tenders for a period to be decided by LIC.	We request that blacklisting be restricted to only matters relating to fraud and corrupt practices.	Please be guided by the RFP
207	7		100	The Vendor will indemnify LIC against all third-party claims of infringement of patent, Intellectual Property Rights, trademark, copy right or industrial design rights arising from use of the Vendor „s Solution or any part thereof throughout the Offices of LIC, including but not limited to the legal actions by any third party against LIC. The LIC shall not be held liable for and would be absolved of any responsibility or claim/litigation arising out of the use of any third-party software or its components or modules supplied by the bidder in terms of requirements of this RFP.	We would request that this clause be amended to amended as follows: "The Vendor will indemnify LIC against all **direct** third-party claims of infringement of patent, Intellectual Property Rights, trademark, copy right or industrial design rights arising from **the permitted and agreed upon** use of the Vendor's Solution or any part thereof throughout the Offices of LIC, including but not limited to the legal actions by any third party against LIC. The LIC shall not be held liable for and would be absolved of any responsibility or claim/litigation arising out of the **the permitted and agreed upon** use of any third-party software or its components or modules supplied by the bidder in terms of requirements of this RFP."	Please be guided by the RFP
208	7		100	In no event shall LIC be liable for any indirect, incidental, or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered. For this purpose, it would be immaterial how such liability may arise, provided that the claims against customers, users, and service providers of LIC are considered as a direct claim	We would request that this clause be made mutual.	Please be guided by the RFP
209	8		100	If Vendor fails to comply any part of the service that does not meet the specifications on three or more occasions, LIC may (in addition to its other remedies) terminate the Contract by giving the Vendor written notice of 15 days.	We would request that the clause be amended as follows, to ensure that we are able to whatever extent possible are able to deliver the services for you: "If Vendor fails to comply any part of the service that does not meet the specifications on three or more occasions, LIC may (in addition to its other remedies) terminate the Contract by giving the Vendor written notice of ~~15~~ **30** days **after the cure period** ."	Please be guided by the RFP
210	8	a	101	LIC may, at any time, by a prior written notice of 30 days, terminate the contract or reduce the scope of the Services.	We would request the notice period be extended to 60 days for cause of convenience to ensure that we are able to account and adjust for the same.	Please be guided by the RFP
211	8		101	Notwithstanding what has been stated in this RFP LIC may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Vendor, terminate the Contract in whole or part if the Vendor fails to deliver any or all of the systems within the period(s) specified in Scope of Work of the RFP, or if the Vendor fails to perform any other obligation(s) under the Contract.	We would request that the clause be amended as follows: "Notwithstanding what has been stated in this RFP LIC may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Vendor, terminate the Contract in whole or part if the Vendor fails to deliver any or all of the systems within the period(s) specified in Scope of Work of the RFP, or if the Vendor fails to perform any other obligation(s) under the Contract, **after a cure period of 30 days and notice have been provided** ."	Notwithstanding what has been stated in this RFP LIC may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Vendor, terminate the Contract in whole or part if the Vendor fails to deliver any or all of the systems within the period(s) specified in Scope of Work of the RFP, or if the Vendor fails to perform any other obligation(s) under the Contract after a cure period of 30 days have been provided in writing .

#	Section	Sub-section	Page	Clause	Query	Response
212	8		101	LIC may, at any time, terminate the Contract by giving written notice to the Vendor, if the Vendor becomes bankrupt or otherwise insolvent. In this event, the termination will be without compensation to the Vendor, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to LIC. In case of termination under this clause LIC is liable to pay for all the services performed by the Vendor till the effective date of termination.	We would humbly submit that by going bankrupt or insolvent, it should not preclude us from receiving payments for services that we have already provided and have been accepted. We would request that the clause be amended as follows: "~~LIC~~ **Either party** may, at any time, terminate the Contract by giving written notice to the other party ~~Vendor~~, if the party ~~Vendor~~ becomes bankrupt or otherwise insolvent. ~~In this event, the termination will be without compensation to the Vendor, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to LIC.~~ In case of termination under this clause LIC is liable to pay for all the services performed by the Vendor till the effective date of termination."	Please be guided by the RFP
213	8		102	The following clauses survive the termination and expiry of the contract: a.Intellectual Property Rights. b.Indemnity. c.Insurance. d.Confidentiality and privacy. e.Protection of personal information. f.Security. g.Audit and access h.Knowledge transfer i.Warranty	We would request that other than confidentiality, protection of personal information, knowledge transfer and warranty (the last two subject to the agreed upon period, that the rest be deleted as these are not survival clauses.	Please be guided by the RFP
214	Annexure K	5	124	LIC need not prove or show grounds or reasons for the demand of a part or the full amount of guarantee.	We would kindly request that this be deleted as it would only be in good conscience that the grounds for demand be provided as well, and for it to not be arbitrary.	Please be guided by the RFP
215	Annexure O		132	LIC need not prove or show grounds or reasons for the demand of a part or the full amount of guarantee.	We would kindly request that this be deleted as it would only be in good conscience that the grounds for demand be provided as well, and for it to not be arbitrary.	Please be guided by the RFP
216	Annexure C: Eligibility Criteria	2	112	The Bidder must have an annual turnover of minimum Rs. 100 Crores per annum during the last 03 (three) years preceding the date of this RFP	Request you to amend to avaerage annual turnover of Rs.40 crores for 3 years	Please be guided by the RFP
217	Annexure C: Eligibility Criteria	4	112	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	Can this be amended to 1 out of 7 solutions?	Please be guided by the RFP
218	Annexure C: Eligibility Criteria	5	112	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different ocations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP	Can the IP count or branches count be reduced?	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
219	Annexure C: Eligibility Criteria	6	112	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Can we submit single experience details?Can you amend the branches count as well?	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
220	Annexure C: Eligibility Criteria	8	113	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Can this be revised to 1 organisations with the amendment in the branches count as well?	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
221	Annexure C: Eligibility Criteria	9	113	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Can this be revised to 1 organisations with the amendment in the branches count as well?	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
222	Annexure C: Eligibility Criteria	11	113	The bidder must have a minimum of 15 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / OEM Level Certification. Minimum 3 resources must have OEM Level Certification (preferably of the proposed OEM).	Please amend the count to minimum 5 resources	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
223	G	Section G: Payment Terms & Conditions	104	Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC.	Please amend this to100% after delivery of software licenses along with invoice	Please refer to the revised "Payment Terms & Conditions"
224	G	Section G: Payment Terms & Conditions	104	Installation and integration, initial OEM audit and acceptance testing as per scope of work.	Please amend this to 50% advance and balance 50% on completion	Please refer to the revised "Payment Terms & Conditions"
225	G	Section G: Payment Terms & Conditions	105	Payment for the Onsite Services will be done on quarterly basis at the end of each quarter	Request to amend payment terms as quarterly in advance	Please be guided by the RFP
226	Annexure F - Technical Compliance VDI Pointers_	40	NA	The solution should be able encrypt end to end traffic from end user to network to controller/broker	Since Broker remains in LAN and connect VDI server in LAN only, the encyption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: **Modified lines should be:** The solution should be able encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"

227	Annexure F - Technical Compliance VDI Pointers_	49	NA	The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders	Expectation in line is not clear, request to add specific requirement as below for clarification. **Modified lines should be:** The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders	Please refer to the revised "Annexure F"
228	Annexure F - Technical Compliance VDI Pointers_	66	NA	The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable	In VDI all computing happended on server using server resource Video will also use server media player for to open video files. however recent adncement has decoupled colaboration tool's audio & video offloading to end-point, please modify and put colaboration tool Audio & Video. Also Flash is no more in use please remove it. **Modified lines should be:** The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and ~~flash content~~ to endpoint when the endpoint is capable	Please refer to the revised "Annexure F"
229	Annexure F - Technical Compliance VDI Pointers_	73	NA	The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing	HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. **Modified lines should be:** The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
230	Annexure F - Technical Compliance VDI Pointers_	76	NA	The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment.	launch time of VDI depends on many factors , like AD, Group ploicy, printer and drive mapping it requires more times than defalt desktop, 5 second login time is unachivable, please modify it to minimum 25 sec. **Modified lines should be:** The solution should be able to provide a launch and access to a virtual application ~~in less than 5~~ between (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
231	Annexure C - Eligibility criteria		Page 113/Sr.No.8	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	The clause implies that the bidders should have implemented proposed OEM VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
232	Section G - Payment Terms & Conditions		Page 104	Point No 3 - Payment schedule table	As we will be supplying perpetual license at the beginning, 100% license cost should be paid once icenses are delivered and invoices raised.	Please refer to the revised "Payment Terms & Conditions"
233	2. Detailed Scope of Work	I. General Requirements	63	The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period. Over the 5-year contract period, bidder may consider an increase of 50% in the number of devices or solutions to be monitored when determining system specifications.	In the sizing requirements for NAC , its advised to refer Tech Specs , point 67 towhich mentions "Total of 127000 endpoint devices and scalable to 160000 devices" above is only 26% and doesnt align with this clause. with 50% increase the scalability ask has to be 191000 , Request this be clarified so the ambiguity doesnt hold	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
234	2. Detailed Scope of Work	I. General Requirements	63	The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Request this be modified as below The bidder / System Integrator shall engage the services of respective OEMs / OEM certified Partner for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Please refer to the revised "Section E: Scope of Services"
235	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall ensure that the OEM(s) has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC"s infrastructure during the tenure of this project.	Request this be modified as below The bidder shall ensure that the OEM(s)/ OEM certified Partener has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC"s infrastructure during the tenure of this project.	Please refer to the revised "Section E: Scope of Services"
236	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder"s resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Request this be modified as below The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM / OEM certified Partner as decided by LIC at the time of implementation. The bidder"s resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM / OEMs certified Partner.	Please refer to the revised "Section E: Scope of Services"
237	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall also engage the services of the respective OEMs for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Request this be modified as below The bidder shall also engage the services of the respective OEMs / OEMs Certified Partner for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Please be guided by the RFP
238	2. Detailed Scope of Work	I. General Requirements	63	The bidder and OEM services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Request this be modified as below The bidder and OEM / OEMs certified Partner services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Please refer to the revised "Section E: Scope of Services"
239	2. Detailed Scope of Work	I. General Requirements	63	The bidder and OEM services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Request this be modified as below The bidder and OEM/OEM certified Partner services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Please refer to the revised "Section E: Scope of Services"

240	2. Detailed Scope of Work	I. General Requirements	64	The vendor should arrange for a comprehensive deployment audit done by OEM after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation.	Request this be changed as The vendor should arrange for a comprehensive deployment audit done by OEM / OEMs certified partner after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation.	Please be guided by the RFP
241	2. Detailed Scope of Work	I. General Requirements	64	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	In the sizing requirements for NAC , its advised to refer Tech Specs , point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices" With 20% YoY growth , the scalability ask should be 263000 , Request this be clarified so the ambiguity doesnt hold and also we inlcude the right breakdown of charges for the additional licenses as ked in this clause	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
242	4. RACI Matrix	2. Network Access Control (NAC)	71	Software Implementation - OEM - A,C	Request this be changes as below Software Implementation - OEM - C	Please refer to the revised "Section E: Scope of Services"
243	4. RACI Matrix	2. Network Access Control (NAC)	71	SLA Performance -OEM- C	Request this be changes as below SLA Performance -OEM- C	Please refer to the revised "Section E: Scope of Services"
244	6. Project Timelines	b. NAC	87	2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. -= T + 5 Weeks= D	Request this be changed to below 2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. -= T + 10 Weeks= D	Please refer to the revised "Section E: Scope of Services"
245	Annexure F: Technical Compliance	NAC #13	119	13. LIC has a hetrogenious network environment comparising network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of any hardware and software	The Network devices should support IEEE 802.1x and Radius COA standards to support NAC.Request if the Netwook devices Make and model be shared , we can thoroughly check and approprriately respond.	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .
246	Annexure F: Technical Compliance	NAC #14	119	The Solution should be compatilbe with the existing network environment of the LIC and any future procurement	while existing network environt is addressed in #13 of the tech specs , we request LIC to procure any routers/switches in future to have support for IEEE 802.1x and Radius COA standards	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .
247	Annexure F: Technical Compliance	NAC #14	119	75 The proposed NAC solution must be in the leaders quadrant in the Gartners magic quadrant for Network Access control in the last published report. This clause will not be applicable for OEMs qualifying under make in India category	Gartner stopped publishing these reports for NAC off late as this solution is matured well , we see the last report as 2019 , request LIC to confirm if the report from 2019 will hold well or let us know if alternate consulting body reports may be considered	Please be guided by the RFP
248	Annexure H: Manufacturer's Authorization Form (MAF)	N/A	121	_ (OEM) certify that, the equipments being sold would not be **declared** End of Support (EoS) in the next 6Years	Request this be rephrased as below since the declaration of End of support and actual EOS of the product is 2 different interpretations _ (OEM) certify that, the equipments being sold would not be End of Support (EoS) in the next 6Years	Please refer to the revised "Annexure H"
249	-	-	Additional point (must have)	The SSLO devices should be STIP compliant.	STIP compliance is part of Common Criteria (CC) that provides a common set of requirements for the security functionality of IT products and the assurance measures to be applied to the IT products during a security evaluation. Does LIC require the SSLO device to be STIP compliant?	Please be guided by the RFP
250	-	-	Additional query	Kindly confirm the total number of applications to be considered for onboarded on SSLO during the deployment phase.	-	Please be guided by the RFP
251	Annexure F - Technical Compliance	API GW	13	The solution should provide features to Convert between different data formats (e.g., JSON to XML).	We request LIC to reconsider older protocol supports like XML is an outdated API protocol, also JSON to XML translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The solution should should provide seamless integration with additional package to Convert between different data formats (e.g., JSON to XML) without adding overheads API-GW solution."	API Gateway and Security Solution has been removed from the scope of this RFP
252	Annexure F - Technical Compliance	API GW	19	The proposed solution should facilitate seamless SOAP to REST transformation, enabling interoperability by translating SOAP-based requests into RESTful API calls, promoting modern integration practices.	We request LIC to reconsider older protocol supports like SOAP is XML based outdated API protocol, also SOAP (XML) to REST (JSON) translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The proposed solution should seamless integration with additional package to translate SOAP to REST, enabling interoperability by translating SOAP-based requests into RESTful API calls as and when required without adding overheads API-GW solution, promoting modern integration practices".	API Gateway and Security Solution has been removed from the scope of this RFP
253	Annexure F - Technical Compliance	API GW	20	The solution should be designed to facilitate a developer organization by providing comprehensive tools, documentation, and support for efficient development.	We request LIC to consider that the mentioned features are getting fulfilled with development tools, not by API gateway, introducing it on API GW will increase overhead and it force developer to restrict themselves to limited features available on such tool. We request LIC to change this clause as: "The solution should be designed to facilitate to integrate it with developer organization by providing compatibility with multiple tools and support for efficient development with the Security of authentication, authorization, payload sanitization and WAF signature inspection"	API Gateway and Security Solution has been removed from the scope of this RFP
254	Annexure F - Technical Compliance	API GW	31	The API gateway should implement streaming APIs using compatible protocols like WebSocket, WebSub, or server-sent events.	We request LIC to kindly change this clause as webSub is a protocol usually used to push content by many websites, including all blogs served by Blogger and WordPress.com news sites. This use case seems to be irrelevant to LIC. Recommended revised clause: "The API gateway should implement streaming APIs using compatible protocols like WebSocket and server-sent events and support WebSub via plugins/packages."	API Gateway and Security Solution has been removed from the scope of this RFP

#	Section	Module	No.	Specification	Query / Suggestion	Response
255	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	3	Device should be based on dedicated <2U hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 4 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 40 vCPUs scalable to 60 vCPU's.	Query: i. RFP has asked for Less than 2RU i.e. 1RU form factor for Propposed appliance, which is not true for all OEM, ii. Amount of vCPU asked on same appliance depends on OEM, as every OEM have different way of working, and different size o CPU which changes the need of numbe rof vCPUs and cannot be binding factor and due to this request to relax the specs **Hence we request to relaxy the requriement to below** Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 2 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 16 CPU	Please refer to the revised "Annexure F"
256	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	4	Should have minimum SSL visibility throughput of 146 Gbps from day 1 and scalable to 195 Gbps on same platform with hardware compression.	**Suggestion:** for the SSLo like technology having such high throughput of 146Gbps Scalable to 195G seems to be overkill **Hence request to change the specs to below:** Should have minimum SSL visibility throughput of 120 Gbps from day 1 on same platform with compression capabilities .	Please refer to the revised "Annexure F" .
257	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	5	Should support minimum SSL Visiblity TPS: -260 K TPS (RSA 2k Keys) from day 1 and scalable to 400 K TPS (RSA 2k Keys) on same platform - 180 K TPS (ECDHE-ECDSA P-256) from day 1 andscalable to 300 K TPS (ECDHE-ECDSA P-256) on same platform	Suggestion: The asked SSL CPS/TPS in the specs seems to be overkill compared to current and future growth and specific to single OEM **Hence request to change the specs to below:** Should support minimum SSL Visiblity TPS: -120 K TPS (RSA 2k keys) from day 1 on same platform - 70 K TPS (ECDHE-ECDSA P-256) from day 1 on same platform	Please refer to the revised "Annexure F" .
258	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR		The SSL Solution should support minimum SSL connections: -L7 requests per second: 6.5 M from day 1 and scalable to 10.5 M on same platform -L4 connections per second: 2.5 M from day 1 andscalable to 3.5 M on same platform -L4 concurrent connections: 350M from day 1	The Asked specs seems to be specific to single OEM **Hence request to change the specs to below** The SSL Solution should support minimum SSL connections: -L7 requests per second: 4M from day 1 -L4 connections per second: 2.5 M from day 1 -L4 concurrent connections: 180M from day 1	Please be guided by the RFP
259	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	6	The SSL solution should have a minimum of 4x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1	Request to change the specs from 4 100/40G ports to 2 100/40G **Hence request to change the specs to below:** The SSL solution should have a minimum of 2x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1	Please be guided by the RFP
260	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR		The SSL Off loader must have the minimum 40 vCPUs from day 1 and scalable to 60 vCPU's on same platform Memory: 512 GB DDR4 Storage: 1 TB SSD	**Suggestion:** Amount of vCPU, Memory and Storage Needed on same appliance depends on OEM, as every OEM have different way of working and cannot be binding factor and **due to this request to relax the specs** **Hence request to relax the specs to below** The SSL Off loader must have the minimum 16 CPU on same platform Memory: 192 GB DDR4 Storage: 500G SSD	Please be guided by the RFP
261	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	7	The proposed solution should have a 45 Gbps bulk encryption from Day 1 and scalable to 100 Gbps bulk encryption	**Suggestion:** Having such high SSL throughput for 100Gbps seems to be overkill **Hence request to change the specs to below:** The proposed solution should have a 45 Gbps bulk encryption from Day 1	Please refer to the revised "Annexure F" .
262	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	14	The SSL offloader solution must support N+1 and 1+1 inline tool redundancy for inline tools.	Feature asked seems to be clustering which is not desired feature for Network appalince due to unpredicable traffic flow and increses troobleshooting complexity **Hence reques to change the specs to below** The SSL offloader solution must support 1+1 inline tool redundancy for inline tools.	Please refer to the revised "Annexure F"
263	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	18	The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same 1RU rack appliance	Having 1RU form factor seems to be specific to single OEM **Hence request to change the specs to below** The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same appliance	Please refer to the revised "Annexure F"

264	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	39	SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration, Zero trust application access with SAML/Oauth with MFA and Secure web gateway (explicity proxy) functionality with add-on licenses if required in future	**Query:** **The features asked in the specs seems to be specific to perticular OEM and below technology seems not to be related to SSLo Solution** - Zero trust application access with SAML/Oauth with MFA - Secure web gateway (explicity proxy) functionality **Hence request to change the specs to below** SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration	Please refer to the revised "Annexure F"
265	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	43	The Proposed solution must provide capabilities to obfuscate sensitive field names in an application to defeat Man-in-The- Browser Attacks on the device itself if required in future via add on licenses	This is specific to a single OEM, hence request to delete the specs	Please refer to the revised "Annexure F"
266	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	79	The SSL Offloader device should have the ability to support C3D	This is specific to a single OEM, hence request to delete the specs	Please be guided by the RFP
267	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	81	The SSL Offloader device should be able to have flexible ICAP request or respond polcies. 1. Enabling ICAP only for HTTP response traffic (It may be useful in some scenarios to only send HTTP response traffic to ICAP, as the vast majority of HTTP GET requests are devoid of payloads.) 2. Enabling ICAP only for HTTP POST request traffic (POST requests will generally always contain a payload, while GET requests usually will not.) 3. Enabling ICAP only for HTTP POST request and all response traffic (This rule will enable ICAP processing on POST requests, all HTTP responses, and would typically be used to filter out normally empty GET and other types of requests.) 4. Enabling ICAP for specific request URL extensions and response content types (Sometimes you just need to activate ICAP for specific file type requests - request URLs that end with something like ".exe", ".sh", or ".bat", and also only scan responses of a specific MIME types (HTTP Content-Type) like "application/json" and application/executable)	**This is specific to a single OEM, hence request to change the specs to below** The SSL Offloader device should be able to have flexible ICAP request or respond polcies.	Please refer to the revised "Annexure F"
268	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	82	The SSL Offloader device should be able to support proxy chaining and act as a explicit forward proxy and following authentication mechanism should be covered 1. Explicit forward proxy authentication 2. Transparent forward proxy authentication (captive portal) 3. Delegate token authentication offload 4. Forward proxy authentication with NTLM 5. Forward proxy authentication with Kerberos	This is specific to a single OEM, hence request to delete the specs	Please be guided by the RFP
269	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	3	Device should be based on dedicated 1U hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 4 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 24 vCPUs scalable to 36 vCPU's.	Query: i. RFP has asked for Less than 2RU i.e. 1RU form factor for Propposed applaiance, which is not true for all OEM, ii. Amount of vCPU asked on same appliance depends on OEM, as every OEM have different way of working, and different size o CPU which changes the need of numbe rof vCPUs and cannot be binding factor and due to this request to relax the specs **Hence we request to relaxy the requriement to below** Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 2 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 16 CPU	Please refer to the revised "Annexure F"
270	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	4	Should have minimum SSL visibility throughput of 115 Gbps from day 1 and scalable to 175 Gbps on same platform with hardware compression.	**Suggestion:** for the SSLo like technology having such high throughput of 146Gbps Scalable to 195G seems to be overkill **Hence request to change the specs to below:** Should have minimum SSL visibility throughput of 120 Gbps from day 1 on same platform with compression capabilities .	Please refer to the revised "Annexure F" .
271	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	5	Should support minimum SSL Visiblity TPS: -100 K TPS (RSA 2k keys) from day 1 and scalable to 180 K TPS (RSA 2k Keys) on same platform - 75 K TPS (ECDHE-ECDSA P-256) from day 1 andscalable to 125 K TPS (ECDHE-ECDSA P-256) on same platform	Suggestion: The asked SSL CPS/TPS in the specs seems to be overkill compared to current and future growth and specific to single OEM **Hence request to change the specs to below**: Should support minimum SSL Visiblity TPS: -120 K TPS (RSA 2k keys) from day 1 on same platform - 70 K TPS (ECDHE-ECDSA P-256) from day 1 on same platform	Please refer to the revised "Annexure F" .
272	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR		The SSL Solution should support minimum SSL connections: -L7 requests per second: 4M from day 1 and scalable to 5.5 M on same platform -L4 connections per second: 1.5 M from day 1 andscalable to 2 M on same platform -L4 concurrent connections: 135M from day 1	The Asked specs seems to be specific to single OEM **Hence request to change the specs to below** The SSL Solution should support minimum SSL connections: -L7 requests per second: 4M from day 1 -L4 connections per second: 2M from day 1 -L4 concurrent connections: 135M from day 1	Please be guided by the RFP

273	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	6	The SSL solution should have a minimum of 4x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1	Request to change the specs from 4 100/40G ports to 2 100/40G **Hence request to change the specs to below:** The SSL solution should have a minimum of 2x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1	Please be guided by the RFP
274	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR		The SSL Off loader must have the minimum 24 vCPUs from day 1 and scalable to 36 vCPU's on same platform Memory: 256GB DDR4 Storage: 1 TB SSD	**Suggestion:** Amount of vCPU, Memory and Storage Needed on same appliance depends on OEM, as every OEM have different way of working and cannot be binding factor and **due to this request to relax the specs** **Hence request to relax the specs to below** The SSL Off loader must have the minimum 16 CPU on same platform Memory: 192 GB DDR4 Storage: 500G SSD	Please be guided by the RFP
275	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	7	The proposed solution should have a 65 Gbps bulk encryption from Day 1 and scalable to 85 Gbps bulk encryption	**Suggestion:** Having such high SSL throughput for 100Gbps seems to be overkill **Hence request to change the specs to below:** The proposed solution should have a 45 Gbps bulk encryption from Day 1	Please be guided by the RFP
276	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	14	The SSL offloader solution must support N+1 and 1+1 inline tool redundancy for inline tools.	Feature asked seems to be clustering which is not desired feature for Network appalince due to unpredicable traffic flow and increses trooubleshooting complexity **Hence reques to change the specs to below** The SSL offloader solution must support 1+1 inline tool redundancy for inline tools.	Please refer to the revised "Annexure F"
277	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	18	The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same 1RU rack appliance	Having 1RU form factor seems to be specific to single OEM **Hence request to change the specs to below** The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same appliance	Please refer to the revised "Annexure F"
278	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	39	SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration, Zero trust application access with SAML/Oauth with MFA and Secure web gateway (explicity proxy) functionality with add-on licenses if required in future	**Query:** **The features asked in the specs seems to be specific to perticular OEM and below technology seems not to be related to SSLo Solution** - Zero trust application access with SAML/Oauth with MFA - Secure web gateway (explicity proxy) functionality **Hence request to change the specs to below** SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration	Please refer to the revised "Annexure F"
279	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	43	The Proposed solution must provide capabilities to obfuscate sensitive field names in an application to defeat Man-in-The- Browser Attacks on the device itself if required in future via add on licenses	This is specific to a single OEM, hence request to delete the specs	Please refer to the revised "Annexure F"
280	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	79	The SSL Offloader device should have the ability to support C3D	This is specific to a single OEM, hence request to delete the specs	Please be guided by the RFP
281	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	81	The SSL Offloader device should be able to have flexible ICAP request or respond polcies. 1. Enabling ICAP only for HTTP response traffic (It may be useful in some scenarios to only send HTTP response traffic to ICAP, as the vast majority of HTTP GET requests are devoid of payloads.) 2. Enabling ICAP only for HTTP POST request traffic (POST requests will generally always contain a payload, while GET requests usually will not.) 3. Enabling ICAP only for HTTP POST request and all response traffic (This rule will enable ICAP processing on POST requests, all HTTP responses, and would typically be used to filter out normally empty GET and other types of requests.) 4. Enabling ICAP for specific request URL extensions and response content types (Sometimes you just need to activate ICAP for specific file type requests - request URLs that end with something like ".exe", ".sh", or ".bat", and also only scan responses of a specific MIME types (HTTP Content-Type) like "application/json" and application/executable)	**This is specific to a single OEM, hence request to change the specs to below** The SSL Offloader device should be able to have flexible ICAP request or respond polcies.	Please refer to the revised "Annexure F"
282	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	82	The SSL Offloader device should be able to support proxy chaining and act as a explicit forward proxy and following authentication mechanism should be covered 1. Explicit forward proxy authentication 2. Transparent forward proxy authentication (captive portal) 3. Delegate token authentication offload 4. Forward proxy authentication with NTLM 5. Forward proxy authentication with Kerberos	This is specific to a single OEM, hence request to delete the specs	Please be guided by the RFP
283	Annexure F - Technical Compliance	WAF Technical specs DC-DR	114	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure	**This is specific to a single OEM, hence request to change the specs to below** The solution must have inbuilt/External bypass segments to ensure that fail open in case of hardware failure	Please be guided by the RFP

284	Annexure F - Technical Compliance	WAF Technical specs NDR	114	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure	**This is specific to a single OEM, hence request to change the specs to below** The solution must have inbuilt/External bypass segments to ensure that fail open in case of hardware failure	Please be guided by the RFP
285	6 Eligibility Criteria	Sr. No. 4	14	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting **minimum 2 out of the 7** in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
286	6 Eligibility Criteria	Sr. No. 5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	We request to revise the criteria as below: "The **bidder / OEM** during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
287	6 Eligibility Criteria	Sr. No. 6	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The **bidder / OEM** during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to **at least 02 (two) organisations** in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
288	6 Eligibility Criteria	Sr. No. 7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The **bidder / OEM** during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least **02 (two)** organisations in PSU / Government / Private / BFSI Sector Firms."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
289	6 Eligibility Criteria	Sr. No. 8	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The **bidder / OEM** during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 01 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
290	6 Eligibility Criteria	Sr. No. 9	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The **bidder / OEM** during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
291	24 Performance Bank Guarantee (PBG)	a)	34	After finalization of the RFP process, the selected bidder should submit an unconditional and irrevocable Performance Bank Guarantee (from a scheduled/ nationalized Public Sector Bank acceptable to LIC and having Branches in Mumbai) equal to 10% of the Total Contract Value.	As per the revised Rule 171(i) of GFR 2017, the performance security should be for an amount of 3 to 10% of contract value. Therfeore, we request you to reduce this Performance Bank Guarantee to 5% of the Total Contract Value.	After finalization of the RFP process, the selected bidder should submit an unconditional and irrevocable Performance Bank Guarantee (from a scheduled/ nationalized Public Sector Bank acceptable to LIC and having Branches in Mumbai) equal to 5% of the Total Contract Value.
292	Section G:	Sr. No. 1	104	Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC. - 30% of Cost	We request to revise the payment clause as below: "Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC. - **70% of Cost**"	Please refer to the revised "Section E: Scope of Services"
293	Section G:	Sr. No. 2	104	Installation and integration, initial OEM audit and acceptance testing as per scope of work. - 40% 0f Cost	We request to revise the payment clause as below: "Installation and integration, initial OEM audit and acceptance testing as per scope of work. - **20% 0f Cost**"	Please refer to the revised "Section E: Scope of Services"
294	Section G:	Sr. No. 3	104	After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s - 25% of Cost	We request to revise the payment clause as below: "After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s - **5% of Cost**"	Please refer to the revised "Section E: Scope of Services"
295	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period. Over the 5-year contract period, bidder may consider an increase of 50% in the number of devices or solutions to be monitored when determining system specifications.	In the sizing requirements for NAC , its advised to refer Tech Specs , point 67 towhich mentions "Total of 127000 endpoint devices and scalable to 160000 devices" above is only 26% and doesnt align with this clause. with 50% increase the scalability ask has to be 191000 , Request this be clarified so the ambiguity doesnt hold	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
296	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Request this be modified as below The bidder / System Integrator shall engage the services of respective OEMs / OEM certified Partner for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Please refer to the revised "Section E: Scope of Services"
297	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The bidder shall ensure that the OEM(s) has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC"s infrastructure during the tenure of this project.	Request this be modified as below The bidder shall ensure that the OEM(s)/ OEM certified Partener has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC"s infrastructure during the tenure of this project.	Please refer to the revised "Section E: Scope of Services"
298	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder"s resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Request this be modified as below The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM / OEM certified Partner as decided by LIC at the time of implementation. The bidder"s resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM / OEMs certified Partner.	Please refer to the revised "Section E: Scope of Services"

299	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The bidder shall also engage the services of the respective OEMs for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Request this be modified as below

The bidder shall also engage the services of the respective OEMs / OEMs Certified Partner for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them. | Please be guided by the RFP |
| 300 | Section E: Scope of Services | 2. Detailed Scope of Work I. General Requirements | 63 | The bidder and OEM services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below: | Request this be modified as below

The bidder and OEM / OEMs certified Partner services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below: | Please refer to the revised "Section E: Scope of Services" |
| 301 | Section E: Scope of Services | 2. Detailed Scope of Work I. General Requirements | 63 | The bidder and OEM services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise. | Request this be modified as below

The bidder and OEM/OEM certified Partner services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise. | Please refer to the revised "Section E: Scope of Services" |
| 302 | Section E: Scope of Services | 2. Detailed Scope of Work I. General Requirements | 64 | The vendor should arrange for a comprehensive deployment audit done by OEM after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation. | Request this be changed as

The vendor should arrange for a comprehensive deployment audit done by OEM / OEMs certified partner after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation. | Please be guided by the RFP |
| 303 | Section E: Scope of Services | 2. Detailed Scope of Work I. General Requirements | 64 | All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth. | In the sizing requirements for NAC , its advised to refer Tech Specs , point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices"

With 20% YoY growth , the scalability ask should be 263000 , Request this be clarified so the ambiguity doesnt hold and also we inlcude the right breakdown of charges for the additional licenses as ked in this clause | Please refer to the revised "Section E: Scope of Services" |
| 304 | Section E: Scope of Services | 4. RACI Matrix | 71 | 2. Network Access Control (NAC) Software Implementation - OEM - A,C | Request this be changes as below

Software Implementation - OEM - C | Please refer to the revised "Section E: Scope of Services" |
| 305 | Section E: Scope of Services | 4. RACI Matrix | 71 | 2. Network Access Control (NAC) SLA Performance -OEM- C | Request this be changes as below

SLA Performance -OEM- C | Please refer to the revised "Section E: Scope of Services" |
| 306 | Section E: Scope of Services | 6. Project Timelines b. NAC | 87 | 2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. -= T + 5 Weeks= D | Request this be changed to below

2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. -= **T + 10 Weeks= D** | Please refer to the revised "Section E: Scope of Services" |
307	Section H: Enclosures	Annexure F: Technical Compliance NAC #13	119	13. LIC has a hetrogenious network environment comparising network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of any hardware and software	The Network devices should support IEEE 802.1x and Radius COA standards to support NAC.Request if the Netwook devices Make and model be shared , we can thoroughly check and approprriately respond.	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .
308	Section H: Enclosures	Annexure F: Technical Compliance NAC #14	119	14.The Solution should be compatilbe with the existing network environment of the LIC and any future procurement	while existing network environt is addressed in #13 of the tech specs , we request LIC to procure any routers/switches in future to have support for IEEE 802.1x and Radius COA standards	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .
309	Section H: Enclosures	Annexure F: Technical Compliance NAC #67	119	67. The Proposed solution should provide comprehensive visiblity of the network by automatically discovering , classifying and enforcing policy for endpoints connected to the network and must have capacity to support the appropriate service for a total of 127000 endpoint devices and scalable to 160000 devices	Request the count of end user devices and the headless devices be please shared out of the asked 127000 now and 160000 devices in future	The details shall be shared with the successful bidder
310	Section H: Enclosures	Annexure F: Technical Compliance NAC #69	119	69. The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001 etc) and any applicable Laws and regulations (such as IRDAI, DPDP Act etc)	while we are ISO27001 complied , DPDP act is not fully mature and may take some time to freeze, we request LIC to remove this and also share the IRDAI Laws and regulations Document to check for compliance	Please refer to the revised "Annexure F"
311	Section H: Enclosures	Annexure F: Technical Compliance NAC #75	119	75. The proposed NAC solution must be in the leaders quadrant in the Gartners magic quadrant for Network Access control in the last published report. This clause will not be applicable for OEMs qualifying under make in India category	Gartner stopped publishing these reports for NAC off late as this solution is matured well , we see the last report as 2019 , request LIC to confirm if the report from 2019 will hold well or let us know if alternate consulting body reports may be considered	Please be guided by the RFP
312	Section H: Enclosures	Annexure H: Manufacturer's Authorizatio n Form (MAF)	121	_ (OEM) certify that, the equipments being sold would not be **declared** End of Support (EoS) in the next 6Years	Request this be rephrased as below since the declaration of End of support and actual EOS of the product is 2 different interpretations

_ (OEM) certify that, the equipments being sold would not be End of Support (EoS) in the next 6Years | Please refer to the revised "Annexure H" |

Sr No	Section/Title	Ref	Page	Clause	Query	Response
313	Queries for Eligibility Criteria	Section B) Eligibaliyu no: 4	14	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We are requesting for..... The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms within different Locationsacross in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
314	Section B) 6 Eligibolity Criteria Point 4)	Section B) Eligiblity Criteria No.5 to no.9	14,15	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	LIC has asked for Four - in scope Solutions out of 7, in E.Criteria no.4, & from criteria No.5 to Criteria no.9 you have asked for 5 individual inscope solutions (No.5# NAC,No..6# WAF,No.7 # MDM/SSLO, No.8.VDI/API Gateway, No.9# CASB.) These are 5- individual solutions, **Kindly confirm on 4 out of 7.** **instead of (5 out of 7).**	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
315	Section B) 6 Eligibolity Criteria Point 9)	Section B) Eligiblity Criteria No.9	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We are requesting to remoove this Criteria, for bidder. (please keep it for Propossed OEM)	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
316	Section B) Eligiblity Criteria No.5	Section B) Eligiblity Criteria No.5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different Locations in India	We are Propssing For:- The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least One organisations in PSU/Government/Private/BFSI Sector Firms different Locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
317	Section B) Eligiblity Criteria No.6	Section B) Eligiblity Criteria No.6	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
318	Section B) Eligiblity Criteria No.7	Section B) Eligiblity Criteria No.7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	WE ARE PROPOSSING FOR:- The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least ONE organisations in PSU / Government / Private / BFSI Sector Firms across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
319	Section B) Eligiblity Criteria No.8	Section B) Eligiblity Criteria No.8	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	WE ARE PROPOSSING FOR :- The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least One organisations in PSU / Government / Private / BFSI Sector Firms across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
320	Annexure F - Technical Compliance VDI Pointers_	40	NA	The solution should be able encrypt end to end traffic from end user to network to controller/broker	Since Broker remains in LAN and connect VDI server in LAN only, the encyption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: **Modified lines should be:** The solution should be able encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"
321	Annexure F - Technical Compliance VDI Pointers_	49	NA	The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders	Expectation in line is not clear, request to add sepecic requirement as below for clarification. **Modified lines should be:** The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders	Please refer to the revised "Annexure F"
322	Annexure F - Technical Compliance VDI Pointers_	66	NA	The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable	In VDI all computing happended on server using server resource Video will also use server media player for to open video files. however recent adncement has decoupled colaboration tool's audio & video offloading to end-point, please modify and put colaboration tool Audio & Video. Also Flash is no more in use please remove it. **Modified lines should be:** The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and flash content to endpoint when the endpoint is capable	Please refer to the revised "Annexure F"
323	Annexure F - Technical Compliance VDI Pointers_	73	NA	The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing	HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. **Modified lines should be:** The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
324	Annexure F - Technical Compliance VDI Pointers_	76	NA	The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment.	launch time of VDI depends on many factors , like AD, Group ploicy, printer and drive mapping it requires more times than defalt desktop, 5 second login time is unachivable, please modify it to minimum 25 sec. **Modified lines should be:** The solution should be able to provide a launch and access to a virtual application in less than 5 between (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
325	Annexure C - Eligibility criteria		Page 113/Sr.No.8	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	The clause implies that the bidders should have implemented proposed OEM VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"

#	Section	Sub	Page	Clause	Query	Response
326	Section G - Payment Terms & Conditions		Page 104	Point No 3 - Payment schedule table	As we will be supplying perpetual license at the beginning, 100% license cost should be paid once icenses are delivered and invoices raised.	Please refer to the revised "Payment Terms & Conditions"
327	6	4	14	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The Bidder should have minimum of 2 years of experience in Implementing or supporting minimum 3 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. Customer do buy directly and prefer SI for implement / support. Request to modify the same.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
328	6	5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	Request to modify to - The bidder during the last 5 years preceding to the date of this RFP should have implemented or supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 01 (one) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. Customer do buy directly and prefer SI for implement / support. Request to modify the same.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
329		6	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 01 (one) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. Customer do buy directly and prefer SI for implement / support. Request to modify the same.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
330		7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 01 (one) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India. Customer do buy directly and prefer SI for implement / support. Request to modify the same.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
331		8	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The bidder / oem during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 01 (one) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India. Customer do buy directly and prefer SI for implement / support. Request to modify the same.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
332		9	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 01 (one) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. Customer do buy directly and prefer SI for implement / support. Request to modify the same.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
333	Scope of Work		55	Support Process Requirement The vendor has to create separate interfaces for them/LIC administrators to carry out the minimum possible jobs, which may be changed as per the business needs ensuring compliance to LIC Security policies. There should be a provision to audit the changes done to fix the accountability.	Need clarity on the separate interface requirements. Is bidder expected to provide any tool for Incident or Change management ?	Please refer to the revised "Section E: Scope of Services"
334	Scope of Work		56	The Vendor has to provide a portal application with authentication to implement, assess and track various trouble-tickets to higher officials of LIC. The site has to be updated regularly by the on-site Personnel	Is Biddder expected to provide any ITSM tool ? If not, need clarity on expectations from bidder. Need clarity on portal application mentioned in the statement.	Please refer to the revised "Section E: Scope of Services"
335	Scope of Work		56	No telephone connection will be provided by LIC to the onsite support persons	We assume here telephone connection refers to mobile phone for the onsite resources . Kindly confirm. We asssume other logistics like seating space, desktop and other admin facilities would be provided by LIC to the onsite resources . Kindly confirm.	Logistics like seating space, desktop and other admin facilities would be provided by LIC to the onsite resources
336	Onsite-support Services	NAC	58	For initial phase 24x7 number of onsite support is required later after the solution is implemented and stable the number of onsite resources for monitoring would be 8x5	What is the expected timeline for 24*7 ? Can we assume 8*5 support 2nd year onward?	Please refer to the revised "Section E: Scope of Services"
337		Mobile Device Management (MDM)	61	On-Site Support shall ensure logical and acceptable conclusion of all the monitoring, management, mitigation, administration, and reporting issues	What is the coverage expected for MDM onsite and remote support ?	Please be guided by the RFP
338	Detail SOW	CASB	NAC	SSLO etc	65	The vendor should offer on-site and remote training for administrators and end-users, as well as remote 8x5 technical support with on-call if required.	Need to understand purpose of this training apart from yearly training asked for each module as part of training section of the RFP document. Request to provide clarity.	Please be guided by the RFP
339	Detail SOW	CASB	NAC	SSLO etc	65	Onsite L3 support is required by LIC during the implementation phase and once the sign-off is provided by LIC the support of L3 will not be further required.	Is bidder need to factor only l1 and l2 onsite support duringt he operation post implementation sign-off ? Request LIC to confirm expectation on L3 support.	Please be guided by the RFP
340	3. Sizing Requirements	All Solutions	70	Sizing Parameters	1. Is HA required to be factored for all solutions ? Please confirm. 2. What all solution among the list shared are new addition or replacement of the existing technologies ?	Please refer to the revised "Section E: Scope of Services"
341	5. Resource Deployment	Project Coordinator	73	Project Coordinator - count 1	1. Is Project coordinator required to be onsite ? 2. What is the expected coverage window?	Please refer to the revised "Section E: Scope of Services"

#	Section	Sub	Page	Clause	Query/Comment	Response
342	5. Resource Deployment	CASB	73	CASB : The L1 resource shall be utilized in a shared mode from the network resource deployment.	Need clarity how to leverage shared resource. What is "Network Resource Deployment ?	Please refer to the revised "Section E: Scope of Services"
343	5. Resource Deployment	NAC | SSLO | WAF | MDM	73-77	L1 and L2 Resource Count - 24*7 Coverage	We undersdtand for each mentioned technology solution bidder to provision 2*L2 and 2*L1 Resources i.e 4 per technology to provide 24*7 onsite support coverage. Kindly confimr if the understanding is correct.	Please refer to the revised "Section E: Scope of Services"
344	5. Resource Deployment	API | VDI	78-80	L1 and L2 Resource - Solution Analyst	Kindly confirm the support coverage. Is it 8*5 support from LIC office ?	Please refer to the revised "Section E: Scope of Services"
345	Onsite Support Services	SUPPORT PROCESS REQUIREMENT:	85	Day-to-day maintenance of the network gateway security setup along with associated appliances like routers, switches, Link load balancers etc. which may be provided by LIC.	Need Clarity on Other components to be managed by Bidder's team. Request LIC team to provide list of components along with the scope.	Please refer to the revised "Section E: Scope of Services"
346	Onsite Support Services	Remote (offsite) Support	86	Remote (offsite) Support	Request LIC to confirm following on Remote Support Ask: 1. Remotye Support Coverage Window ? 2. Number of Resources per technology for remote support 3. Scope of Remote Support Team for each technology	Please refer to the revised "Section E: Scope of Services"
347	Onsite Support Services	Service-Delivery and Project Management	86	The selected vendor will have to post a full-time onsite Service-Delivery Manager (SDM) immediately after the signing of the Contrac	Is Project coordinator and Service Delivery manager Same or Bidder need to factor separate Project coordinator and Service Delioery Manager ?	Please refer to the revised "Section E: Scope of Services"
348	3. Sizing Requirements	All Solutions	70	Sizing Parameters	1. Reuqets LIC to share the Application inventory to be onbaorded on WAF/API 2. Reuqest LIC to share the one time implementation scope for each technology	Please refer to the revised "Section E: Scope of Services"
349	Section C	Anexxure R	19		Quantity of WAF gateways and Management systems are not mentioned in Annexure R Bill of Quantity	Please refer to the revised "Section E: Scope of Services"
350	Section H	Annexure F, 10		For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authentcated via RADIUS, TACACS+ or via local tabel of authorized users.	Request to modify the clause as "For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authentcated via RADIUS/ TACACS+ / via local table of authorized users."	Please refer to the revised "Annexure F"
351	Section H	Annexure F, 86		The solution must protect system against WASC Wec Security Attack classification.	Request to modify the clasue as "The solution must protect system against WASC Wec Security Attack classification or OWASP top 10."	Please refer to the revised "Annexure F"
352		Compliance			The CASB Solution must have HTTP/2 support from day 1.	Please refer to the revised "Annexure F"
353		Compliance			The CASB Solution must have 99% uptime SLA	Please refer to the revised "Annexure F"
354		Compliance			The solution must have Web IPS (Signatures) to protect against targeted user-agent threats	Please refer to the revised "Annexure F"
355	Annexure F - Technical Compliance	API GW	13	The solution should provide features to Convert between different data formats (e.g., JSON to XML).	We request LIC to reconsider older protocol supports like XML is an outdated API protocol, also JSON to XML translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The solution should should provide seamless integration with additional package to Convert between different data formats (e.g., JSON to XML) without adding overheads API-GW solution."	API Gateway and Security Solution has been removed from the scope of this RFP
356	Annexure F - Technical Compliance	API GW	19	The proposed solution should facilitate seamless SOAP to REST transformation, enabling interoperability by translating SOAP-based requests into RESTful API calls, promoting modern integration practices.	We request LIC to reconsider older protocol supports like SOAP is XML based outdated API protocol, also SOAP (XML) to REST (JSON) translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The proposed solution should seamless integration with additional package to translate SOAP to REST, enabling interoperability by translating SOAP-based requests into RESTful API calls as and when required without adding overheads API-GW solution, promoting modern integration practices".	API Gateway and Security Solution has been removed from the scope of this RFP
357	Annexure F - Technical Compliance	API GW	20	The solution should be designed to facilitate a developer organization by providing comprehensive tools, documentation, and support for efficient development.	We request LIC to consider that the mentioned features are getting fulfilled with development tools, not by API gateway, introducing it on API GW will increase overhead and it force developer to restrict themselves to limited features available on such tool. We request LIC to change this clause as: "The solution should be designed to facilitate to integrate it with developer organization by providing compatibility with multiple tools and support for efficient development with the Security of authentication, authorization, payload sanitization and WAF signature inspection"	API Gateway and Security Solution has been removed from the scope of this RFP
358	Annexure F - Technical Compliance	API GW	31	The API gateway should implement streaming APIs using compatible protocols like WebSocket, WebSub, or server-sent events.	We request LIC to kindly change this clause as webSub is a protocol usually used to push content by many websites, including all blogs served by Blogger and WordPress.com news sites. This use case seems to be irrelevant to LIC. Recommended revised clause: "The API gateway should implement streaming APIs using compatible protocols like WebSocket and server-sent events and support WebSub via plugins/packages."	API Gateway and Security Solution has been removed from the scope of this RFP
359			Additional point (must have)	The SSLO devices should be STIP compliant.	STIP compliance is part of Common Criteria (CC) that provides a common set of requirements for the security functionality of IT products and the assurance measures to be applied to the IT products during a security evaluation. Does LIC require the SSLO device to be STIP compliant?	Please be guided by the RFP
360			Additional query	Kindly confirm the total number of applications to be considered for onboarded on SSLO during the deployment phase.	-	Please be guided by the RFP
361	2. Detailed Scope of Work	I. General Requirements	63	The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period. Over the 5-year contract period, bidder may consider an increase of 50% in the number of devices or solutions to be monitored when determining system specifications.	In the sizing requirements for NAC , its advised to refer Tech Specs , point 67 towhich mentions "Total of 127000 endpoint devices and scalable to 160000 devices" above is only 26% and doesnt align with this clause. with 50% increase the scalability ask has to be 191000 , Request this be clarified so the ambiguity doesnt hold	Please refer to the revised "Section E: Scope of Services"

#	Section	Subsection	Page	Original Text	Request	Response
362	2. Detailed Scope of Work	I. General Requirements	63	The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Request this be modified as below The bidder / System Integrator shall engage the services of respective OEMs / OEM certified Partner for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Please refer to the revised "Section E: Scope of Services"
363	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall ensure that the OEM(s) has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Request this be modified as below The bidder shall ensure that the OEM(s)/ OEM certified Partener has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Please refer to the revised "Section E: Scope of Services"
364	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder"s resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Request this be modified as below The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM / OEM certified Partner as decided by LIC at the time of implementation. The bidder"s resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM / OEMs certified Partner.	Please refer to the revised "Section E: Scope of Services"
365	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall also engage the services of the respective OEMs for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Request this be modified as below The bidder shall also engage the services of the respective OEMs / OEMs Certified Partner for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Please refer to the revised "Section E: Scope of Services"
366	2. Detailed Scope of Work	I. General Requirements	63	The bidder and OEM services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Request this be modified as below The bidder and OEM / OEMs certified Partner services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Please refer to the revised "Section E: Scope of Services"
367	2. Detailed Scope of Work	I. General Requirements	63	The bidder and OEM services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Request this be modified as below The bidder and OEM/OEM certified Partner services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Please refer to the revised "Section E: Scope of Services"
368	2. Detailed Scope of Work	I. General Requirements	64	The vendor should arrange for a comprehensive deployment audit done by OEM after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation.	Request this be changed as The vendor should arrange for a comprehensive deployment audit done by OEM / OEMs certified partner after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation.	Please refer to the revised "Section E: Scope of Services"
369	2. Detailed Scope of Work	I. General Requirements	64	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	In the sizing requirements for NAC , its advised to refer Tech Specs , point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices" With 20% YoY growth , the scalability ask should be 263000 , Request this be clarified so the ambiguity doesnt hold and also we inlcude the right breakdown of charges for the additional licenses as ked in this clause	Please refer to the revised "Section E: Scope of Services"
370	4. RACI Matrix	2. Network Access Control (NAC)	71	Software Implementation - OEM - A,C	Request this be changes as below Software Implementation - OEM - C	Please refer to the revised "Section E: Scope of Services"
371	4. RACI Matrix	2. Network Access Control (NAC)	71	SLA Performance -OEM- C	Request this be changes as below SLA Performance -OEM- C	Please refer to the revised "Section E: Scope of Services"
372	6. Project Timelines	b. NAC	87	2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. -= T + 5 Weeks= D	Request this be changed to below 2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. -= **T + 10 Weeks= D**	Please refer to the revised "Section E: Scope of Services"
373	Section G: Payment Terms & Conditions		104	Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC. - 30% Installation and integration, initial OEM audit and acceptance testing as per scope of work.- 40% After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s - 25% Training/knowledge transfer, documentation of entire solution at specified locations as per the scope of work. - 5%	Request to change as follows - Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC. - 50% Installation and integration, initial OEM audit and acceptance testing as per scope of work.- 30% After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s - 15% Training/knowledge transfer, documentation of entire solution at specified locations as per the scope of work. - 5%	Please refer to the revised "Section E: Scope of Services"
374	Annexure F: Technical Compliance	NAC #67	119	67. The Proposed solution should provide comprehensive visiblity of the network by automatically discovering , classifying and enforcing policy for endpoints connected to the network and must have capacity to support the appropriate service for a total of 127000 endpoint devices and scalable to 160000	Request the count of end user devices and the headless devices be please shared out of the asked 127000 now and 160000 devices in future	The details shall be shared with the successful bidder
375	Annexure F: Technical Compliance	NAC #69	119	69. The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001 etc) and any applicable Laws and regulations (such as IRDAI, DPDP Act etc)	while we are ISO27001 complied , DPDP act is not fully mature and may take some time to freeze, we request LIC to remove this and also share the IRDAI Laws and regulations Document to check for compliance	Please refer to the revised "Annexure F"
376	Annexure F: Technical Compliance	NAC #13	119	13. LIC has a hetrogenious network environment comparising network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of any hardware and software	The Network devices should support IEEE 802.1x and Radius COA standards to support NAC.Request if the Netwook devices Make and model be shared , we can thoroughly check and approprriately respond.	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .

#	Section	Ref	Page/Clause	Clause	Query / Remark	Response
377	Annexure F: Technical Compliance	NAC #14	119	The Solution should be compatilbe with the existing network environment of the LIC and any future procurement	while existing network environt is addressed in #13 of the tech specs , we request LIC to procure any routers/switches in future to have support for IEEE 802.1x and Radius COA standards	Network Devices in LICs Network are managed devices from different OEMS. The complete details shall be provided to the succesful bidder .
378	Annexure F: Technical Compliance	NAC #14	119	75 The proposed NAC solution must be in the leaders quadrant in the Gartners magic quadrant for Network Access control in the last published report. This clause will not be applicable for OEMs qualifying under make in India category	Gartner stopped publishing these reports for NAC off late as this solution is matured well , we see the last report as 2019 , request LIC to confirm if the report from 2019 will hold well or let us know if alternate consulting body reports may be considered	Please be guided by the RFP
379	Annexure H: Manufacturer's Authorization Form (MAF)	N/A	121	_ (OEM) certify that, the equipments being sold would not be **declared** End of Support (EoS) in the next 6Years	Request this be rephrased as below since the declaration of End of support and actual EOS of the product is 2 different interpretations _ (OEM) certify that, the equipments being sold would not be End of Support (EoS) in the next 6Years	Please refer to the revised "Annexure H"
380	Annexure F - Technical Compliance VDI Pointers_	40	NA	The solution should be able encrypt end to end traffic from end user to network to controller/broker	Since Broker remains in LAN and connect VDI server in LAN only, the encyption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: Modified lines should be: The solution should be able encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"
381	Annexure F - Technical Compliance VDI Pointers_	49	NA	The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders	Expectation in line is not clear, request to add sepecific requirement as below for clarification. Modified lines should be: The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders	Please refer to the revised "Annexure F"
382	Annexure F - Technical Compliance VDI Pointers_	66	NA	The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable	In VDI all computing happended on server using server resource Video will also use server media player for to open video files. however recent adncement has decoupled colaboration tool's audio & video offloading to end-point, please modify and put colaboration tool Audio & Video. Also Flash is no more in use please remove it. Modified lines should be: The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and flash content to endpoint when the endpoint is capable	Please refer to the revised "Annexure F"
383	Annexure F - Technical Compliance VDI Pointers_	73	NA	The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing	HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. Modified lines should be: The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
384	Annexure F - Technical Compliance VDI Pointers_	76	NA	The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment.	launch time of VDI depends on many factors , like AD, Group ploicy, printer and drive mapping it requires more times than defalt desktop, 5 second login time is unachivable, please modify it to minimum 25 sec. Modified lines should be: The solution should be able to provide a launch and access to a virtual application in less than 5 between (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
385	Annexure C - Eligibility criteria		Page 113/Sr.No.8	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	The clause implies that the bidders should have implemented proposed OEM VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
386	Eligibility Criteria	Eligibility Criteria	14	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	As multiple Pre-qualification criteria over another is narrowing participation. Hence, we request LIC to consider below clause. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 15,000 IP Addresses to at least 01 (two) organisations in PSU/Government/Private/BFSI Sector Firms. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
387	Eligibility Criteria	Eligibility Criteria	14	6. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request LIC to remove restriction of 500 Branches as it may not be relevantly applicable to PSU/Government 6. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"

388	Eligibility Criteria	Eligibility Criteria	14	7. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	As multiple Pre-qualification criteria over another is narrowing participation. Hence, we request LIC to consider below clause.

The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 01 (two) organisations in PSU / Government / Private / BFSI Sector Firms. | Please refer to the revised "Annexure C and Minimum Eligibility Criteria" |
| 389 | Eligibility Criteria | Eligibility Criteria | 14 | 8. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India | Request LIC to consider below clause

8. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users /API Protection & Discovery - Access Control/ API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms | Please refer to the revised "Annexure C and Minimum Eligibility Criteria" |
| 390 | Eligibility Criteria | Eligibility Criteria | 14 | 9. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. | Request LIC to consider below clause

9. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB)/DLP to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms | Please refer to the revised "Annexure C and Minimum Eligibility Criteria" |
| 391 | Eligibility Criteria | Eligibility Criteria | 14 | The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. | Request LIC to change - The Bidder should have minimum of 3 years of experience in supplying, implementing, or supporting minimum 3 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms across different locations in India. | Please refer to the revised "Annexure C and Minimum Eligibility Criteria" |
| 392 | Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters | Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters | 115 | The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.
⦿ Greater than 7 Years -> 10 Marks
⦿ Greater than 5 Years up to 7 Years -> 7 Marks
⦿ Greater than 3 Years up to 5 Years -> 5 Marks
(Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work) | Request you LIC to consider below technical scoring clause

The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms

⦿ Greater than 7 Years -> 10 Marks
⦿ Greater than 5 Years up to 7 Years -> 7 Marks
⦿ Greater than 3 Years up to 5 Years -> 5 Marks
(Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work) | Please refer to the revised "Annexure C and Minimum Eligibility Criteria" |
| 393 | Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters | Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters | 115 | 3. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of:
⦿ 2 references of 65000 IP Addresses and above -> 10 Marks
⦿ 2 references of 50000 IP Addresses and above -> 7 Marks
⦿ 2 references of 25000 IP Addresses and above -> 5 Marks
(Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work) | Request you LIC to consider below technical scoring clause

3. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of:
⦿ 2 references of 15000 IP Addresses and above -> 10 Marks
⦿ 2 references of 10000 IP Addresses and above -> 7 Marks
⦿ 2 references of 5000 IP Addresses and above -> 5 Marks
(Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work) | Please refer to the revised "Annexure C and Minimum Eligibility Criteria" |
| 394 | Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters | Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters | 115 | 4. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of:
⦿ 3 references and above -> 10 Marks
⦿ 2 references and above -> 5 Marks
(Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work) | Request you LIC to consider below technical scoring clause

4. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of:
· 3 references and above -> 10 Marks
· 2 references and above -> 5 Marks
(Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work) | Please refer to the revised "Annexure C and Minimum Eligibility Criteria" |
| 395 | Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters | Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters | 115 | The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of:
⦿ 3 references and above -> 10 Marks
2 references and above -> 5 Marks
(Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work) | Request you LIC to consider below technical scoring clause

The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader/NGFW/Webproxy solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of:
⦿ 3 references and above -> 10 Marks
2 references and above -> 5 Marks
(Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work) | Please refer to the revised "Annexure C and Minimum Eligibility Criteria" |

#	Section	Sub-Section	Page/Sr No	Clause	Query	Response
396	Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters	Annexure D: Technical Scoring Technical Evaluation Criteria – Parameters	115	6 The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ☐ 2 references of 10000 users and above -> 10 Marks ☐ 2 references of 5000 users and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you LIC to consider below technical scoring clause 6 The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ☐ 2 references of 5000 users and above -> 10 Marks ☐ 2 references of 3000 users and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
397	Annexure F - Technical Compliance VDI Pointers_		40	NA	The solution should be able encrypt end to end traffic from end user to network to controller/broker	Since Broker remains in LAN and connect VDI server in LAN only, the encyption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: **Modified lines should be:** The solution should be able encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"
398	Annexure F - Technical Compliance VDI Pointers_		49	NA	The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders	Expectation in line is not clear, request to add sepecic requirement as below for clarification. **Modified lines should be:** The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders	Please refer to the revised "Annexure F"
399	Annexure F - Technical Compliance VDI Pointers_		66	NA	The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable	In VDI all computing happended on server using server resource Video will also use server media player for to open video files. however recent adncement has decoupled colaboration tool's audio & video offloading to end-point, please modify and put colaboration tool Audio & Video. Also Flash is no more in use please remove it. **Modified lines should be:** The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and ~~flash content~~ to endpoint when the endpoint is capable	Please refer to the revised "Annexure F"
400	Annexure F - Technical Compliance VDI Pointers_		73	NA	The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing	HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. **Modified lines should be:** The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
401	Annexure F - Technical Compliance VDI Pointers_		76	NA	The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment.	launch time of VDI depends on many factors , like AD, Group ploicy, printer and drive mapping it requires more times than defalt desktop, 5 second login time is unachivable, please modify it to minimum 25 sec. **Modified lines should be:** The solution should be able to provide a launch and access to a virtual application ~~in less than 5~~ between (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
402	Annexure C - Eligibility criteria		Page 113/Sr.No.8	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	The clause implies that the bidders should have implemented **proposed OEM** VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
403	Section G - Payment Terms & Conditions		Page 104	Point No 3 - Payment schedule table	As we will be supplying perpetual license at the beginning, 100% license cost should be paid once icenses are delivered and invoices raised.	Please refer to the revised "Payment Terms & Conditions"
404		Eligibility Criteria			LIC To accept 100% owned subsidiary experience & work orders	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
405	Annexure C: Eligibility Criteria	Eligibility Criteria	112	The bidder should be in operating-profit (EBITDA i.e., Earnings before Interest, Tax, Depreciation & Amortization) during the last 03 (three) years preceding the date of this RFP or The bidder should have made profit (before tax) in any of the 03 (three) out of last 05 (five) financial years preceding the date of this RFP and should be having positive net worth for the last 03 (three) financial years preceding to the date of this RFP.	The bidder should be in operating-profit (EBITDA i.e., Earnings before Interest, Tax, Depreciation & Amortization) during the last 03 (three) years preceding the date of this RFP or The bidder should have made profit (before tax) in any of the 02 (two) out of last 03 (three) financial years preceding the date of this RFP and should be having positive net worth for the last 03 (three) financial years preceding the date of this RFP.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
406	Annexure C: Eligibility Criteria	Eligibility Criteria	112	4. The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	Request to modify the clause as: 4. The Bidder or bidder's parent company (incase bidder is wholly owned subsidiary of its parent company) should have minimum of 3 years of experience in supplying, implementing, and supporting **minimum 3** out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
407	Annexure C: Eligibility Criteria	Eligibility Criteria	112	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the clause as: 5. The bidder or BIDDER'S PARENT COMPANY during the last 7 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"

					Request/Modification	Response
408	Annexure C: Eligibility Criteria	Eligibility Criteria	112	6.The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the clause as: 6.The bidder or BIDDER'S PARENT COMPANY during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
409	Annexure C: Eligibility Criteria	Eligibility Criteria	112	7. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the clause as: 7. The bidder or BIDDER'S PARENT COMPANY during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
410	Annexure C: Eligibility Criteria	Eligibility Criteria	112	8. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the clause as: 8. The bidder or BIDDER'S PARENT COMPANY/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
411	Annexure C: Eligibility Criteria	Eligibility Criteria	112	9.The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	9.The bidder /OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
412	Annexure C: Eligibility Criteria	Eligibility Criteria	112	10. The bidder must have a minimum of 15 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / OEM Level Certification. Minimum 3 resources must have OEM Level Certification (preferably of the proposed OEM).	10. The bidder must have a minimum of 15 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / OEM Level Certification. Minimum 3 resources must have OEM Level Certification (preferably any or combination of the proposed OEM).	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
413	Annexure D: Technical Scoring	Annexure D: Technical Scoring	115	The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. ⬜ Greater than 7 Years -> 10 Marks ⬜ Greater than 5 Years up to 7 Years -> 7 Marks ⬜ Greater than 3 Years up to 5 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company/OEM should have relevant implementation and operational experience for similar SOC security tools to PSU/Government/Private/BFSI Sector Firms in India. ⬜ Greater than 7 Years -> 10 Marks ⬜ Greater than 5 Years up to 7 Years -> 7 Marks ⬜ Greater than 3 Years up to 5 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
414	Annexure D: Technical Scoring	Annexure D: Technical Scoring	115	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬜ 2 references of 65000 IP Addresses and above -> 10 Marks ⬜ 2 references of 50000 IP Addresses and above -> 7 Marks ⬜ 2 references of 25000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request to modify the clause : The Bidder or Bidder's Parent company or OEM during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for minimum of: ⬜ 2 references of 25000 IP Addresses and above -> 10 Marks ⬜ 2 references of 10000 IP Addresses and above -> 7 Marks ⬜ 2 references of 5000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
415	Annexure D: Technical Scoring	Annexure D: Technical Scoring	115	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬜ 3 references and above -> 10 Marks ⬜ 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for minimum of: ⬜ 3 references and above -> 10 Marks ⬜ 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
416	Annexure D: Technical Scoring	Annexure D: Technical Scoring	115	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬜ 3 references and above -> 10 Marks ⬜ 2 references and above -> 5 Marks	Kindly modify the clause as: The bidder or bidder's parent company /OEM during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution or extreme SSL aceleration upgrades to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬜ 3 references and above -> 10 Marks ⬜ 2 references and above -> 5 Marks	Please refer to the revised "Annexure D"
417	Annexure D: Technical Scoring	Annexure D: Technical Scoring	116	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬜ 2 references of 10000 users and above -> 10 Marks ⬜ 2 references of 5000 users and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⬜ 2 references of 5000 users and above -> 10 Marks ⬜ 2 references of 5000 users and above -< 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
418	Annexure D: Technical Scoring	Annexure D: Technical Scoring	116	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⬜ 4 references -> 10 Marks ⬜ 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms in India ⬜ 4 references -> 10 Marks ⬜ 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"

419	Annexure D: Technical Scoring	Annexure D: Technical Scoring	116	The bidder must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⬚ 4 references -> 5 Marks ⬚ 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⬚ 4 references -> 5 Marks ⬚ 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
420	Annexure D: Technical Scoring	Annexure D: Technical Scoring	116	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⬚ 4 references -> 5 Marks ⬚ 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⬚ 4 references -> 5 Marks ⬚ 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
421	1. Brief Scope of Work	Planning	50	Ensure compatibility and interoperability between different security solutions.	Kindly provide the details of existing security solution to verify the compatibility and interoperability.	The details shall be shared with the successful bidder
422	1. Brief Scope of Work	Compliance with IS Security Policy	53	o Physical Security of the facilities	Kindly elaborate this as physical security should be in LIC scope.	Please be guided by the RFP
423	1. Brief Scope of Work	Training & Certification	54	Bidder shall train specified LIC employees for operational Management of the system. Training shall be provided on each of the following modules to specified LIC personnel. Training shall be provided at no additional cost to LIC through OEM approved Authorized agencies/faculties. All trainings have to be imparted at LIC's premises.	Kindly provide the number of batches and size of batch for training.	Please refer to the revised "Section E: Scope of Services"
424	1. Brief Scope of Work	Mobile Device Management (MDM)	59	Create, update, and delete access control rules, groups, and policies in WAF after obtaining approval.	We understand that this is related to WAF section not the MDM. Please confirm	Please refer to the revised "Section E: Scope of Services"
425	1. Brief Scope of Work	API Gateway, Management and Security	62	On-Site Support must ensure a smooth handover of these devices from current vendor in specified and declared timelines with proper project management.	Kindly clarify if we need to manage existing API security gateway solution.	API Gateway and Security Solution has been removed from the scope of this RFP
426	2. Detailed Scope of Work	I. General Requirements	62	All the solutions should be seamlessly integrated with the LIC"s NTP solution and must be compatible with any provided NTP version.	Request to provide existing NTP details for integration validation.	The details shall be shared with the successful bidder
427	2. Detailed Scope of Work	II. Cloud Access Security Broker (CASB)	65	The vendor should provide services including data loss prevention (DLP), threat detection, encryption, access control, and compliance monitoring.	Kindly clarify if we need to provide DLP solution along with CASB solution.	Please be guided by the RFP
428	2. Detailed Scope of Work	VIII. Mobile Device Management (MDM)	69	The vendor should deploy API Gateway, Management and Security solution within the organization's network.	We understand that this is related to API Gateway section not the MDM. Please confirm	Please refer to the revised "Section E: Scope of Services"
429	5. Resource Deployment	Project Coordinator	73		Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"
430	5. Resource Deployment	Network Access Control (NAC)	73	L2 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
431	5. Resource Deployment	Network Access Control (NAC)	73	L1 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
432	5. Resource Deployment	SSL Offloader	74	L2 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
433	5. Resource Deployment	SSL Offloader	75	L1 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
434	5. Resource Deployment	Web Application Firewall (WAF)	76	L2 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
435	5. Resource Deployment	Web Application Firewall (WAF)	76	L1 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
436	5. Resource Deployment	Mobile Device Management (MDM)	77	L2 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"

437	5. Resource Deployment	Mobile Device Management (MDM)	77	L1 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"
438	5. Resource Deployment	API Gateway, Management and Security	78	L2 Security Analyst – 1 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	API Gateway and Security Solution has been removed from the scope of this RFP
439	5. Resource Deployment	API Gateway, Management and Security	79	L1 Security Analyst – 1 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	API Gateway and Security Solution has been removed from the scope of this RFP
440	5. Resource Deployment	Virtual Desktop Interface (VDI)	80	L2 Security Analyst – 1 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"
441	5. Resource Deployment	Virtual Desktop Interface (VDI)	80	L1 Security Analyst – 1 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"
442	5. Resource Deployment	Remote (offsite) Support	86	The successful Bidder has to provide throughout the contract period, the services of an offsite support beyond LIC"s office hours. The roles and responsibilities of offsite support would be the same as that of onsite support as mentioned above.	Kindly clarify Remote support person need to be dedicated or shared resource	Please refer to the revised "Section E: Scope of Services"
443	5. Resource Deployment	Remote (offsite) Support	86	The offsite support has to monitor using the VPN setup at vendor end at vendors cost.	We understand that LIC will provide VPN access via SSL client for remote monitoring. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
444	Annexure F - Technical Compliance VDI Pointers_	40	NA	The solution should be able encrypt end to end traffic from end user to network to controller/broker	Since Broker remains in LAN and connect VDI server in LAN only, the encyption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: **Modified lines should be:** The solution should be able encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"
445	Annexure F - Technical Compliance VDI Pointers_	49	NA	The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders	Expectation in line is not clear, request to add sepecic requirement as below for clarification. **Modified lines should be:** The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders	Please refer to the revised "Annexure F"
446	Annexure F - Technical Compliance VDI Pointers_	66	NA	The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable	In VDI all computing happended on server using server resource Video will also use server media player for to open video files. however recent adncement has decoupled colaboration tool's audio & video offloading to end-point, please modify and put colaboration tool Audio & Video. Also Flash is no more in use please remove it. **Modified lines should be:** The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and ~~flash content~~ to endpoint when the endpoint is capable	Please refer to the revised "Annexure F"
447	Annexure F - Technical Compliance VDI Pointers_	73	NA	The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing	HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. **Modified lines should be:** The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
448	Annexure F - Technical Compliance VDI Pointers_	76	NA	The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment.	launch time of VDI depends on many factors , like AD, Group ploicy, printer and drive mapping it requires more times than defalt desktop, 5 second login time is unachivable, please modify it to minimum 25 sec. **Modified lines should be:** The solution should be able to provide a launch and access to a virtual application ~~in less than 5~~ between (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
449	Annexure C - Eligibility criteria		Page 113/Sr.No.8	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	The clause implies that the bidders should have implemented proposed OEM VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
450	Section G - Payment Terms & Conditions		Page 104	Point No 3 - Payment schedule table	As we will be supplying perpetual license at the beginning, 100% license cost should be paid once icenses are delivered and invoices raised.	Please refer to the revised "Payment Terms & Conditions"

451	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	3	Device should be based on dedicated <2U hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 4 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 40 vCPUs scalable to 60 vCPU's.	Query: i. RFP has asked for Less than 2RU i.e. 1RU form factor for Propposed appliance, which is not true for all OEM, ii. Amount of vCPU asked on same appliance depends on OEM, as every OEM have different way of working, and different size o CPU which changes the need of numbe rof vCPUs and cannot be binding factor and due to this request to relax the specs **Hence we request to relaxy the requriement to below** Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 2 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 16 CPU	Please refer to the revised "Annexure F"
452	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	4	Should have minimum SSL visibility throughput of 146 Gbps from day 1 and scalable to 195 Gbps on same platform with hardware compression.	**Suggestion:** for the SSLo like technology having such high throughput of 146Gbps Scalable to 195G seems to be overkill **Hence request to change the specs to below:** Should have minimum SSL visibility throughput of 120 Gbps from day 1 on same platform with compression capabilities .	Please refer to the revised "Annexure F"
453	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	5	Should support minimum SSL Visiblity TPS: -260 K TPS (RSA 2k Keys) from day 1 and scalable to 400 K TPS (RSA 2k Keys) on same platform - 180 K TPS (ECDHE-ECDSA P-256) from day 1 andscalable to 300 K TPS (ECDHE-ECDSA P-256) on same platform	Suggestion: The asked SSL CPS/TPS in the specs seems to be overkill compared to current and future growth and specific to single OEM **Hence request to change the specs to below**: Should support minimum SSL Visiblity TPS: -120 K TPS (RSA 2k keys) from day 1 on same platform - 70 K TPS (ECDHE-ECDSA P-256) from day 1 on same platform	Please refer to the revised "Annexure F"
454	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR		The SSL Solution should support minimum SSL connections: -L7 requests per second: 6.5 M from day 1 and scalable to 10.5 M on same platform -L4 connections per second: 2.5 M from day 1 andscalable to 3.5 M on same platform -L4 concurrent connections: 350M from day 1	The Asked specs seems to be specific to single OEM **Hence request to change the specs to below** The SSL Solution should support minimum SSL connections: -L7 requests per second: 4M from day 1 -L4 connections per second: 2.5 M from day 1 -L4 concurrent connections: 180M from day 1	Please be guided by the RFP
455	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	6	The SSL solution should have a minimum of 4x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1	Request to change the specs from 4 100/40G ports to 2 100/40G **Hence request to change the specs to below:** The SSL solution should have a minimum of 2x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1	Please be guided by the RFP
456	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR		The SSL Off loader must have the minimum 40 vCPUs from day 1 and scalable to 60 vCPU's on same platform Memory: 512 GB DDR4 Storage: 1 TB SSD	**Suggestion:** Amount of vCPU, Memory and Storage Needed on same appliance depends on OEM, as every OEM have different way of working and cannot be binding factor and **due to this request to relax the specs** **Hence request to relax the specs to below** The SSL Off loader must have the minimum 16 CPU on same platform Memory: 192 GB DDR4 Storage: 500G SSD	Please refer to the revised "Annexure F"
457	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	7	The proposed solution should have a 45 Gbps bulk encryption from Day 1 and scalable to 100 Gbps bulk encryption	**Suggestion:** Having such high SSL throughput for 100Gbps seems to be overkill **Hence request to change the specs to below:** The proposed solution should have a 45 Gbps bulk encryption from Day 1	Please refer to the revised "Annexure F"
458	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	14	The SSL offloader solution must support N+1 and 1+1 inline tool redundancy for inline tools.	Feature asked seems to be clustering which is not desired feature for Network appalince due to unpredicable traffic flow and increses troobleshooting complexity **Hence reques to change the specs to below** The SSL offloader solution must support 1+1 inline tool redundancy for inline tools.	Please refer to the revised "Annexure F"
459	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	18	The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same 1RU rack appliance	Having 1RU form factor seems to be specific to single OEM **Hence request to change the specs to below** The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same appliance	Please refer to the revised "Annexure F"

460	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	39	SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration, Zero trust application access with SAML/Oauth with MFA and Secure web gateway (explicity proxy) functionality with add-on licenses if required in future	**Query:** **The features asked in the specs seems to be specific to perticular OEM and below technology seems not to be related to SSLo Solution** - Zero trust application access with SAML/Oauth with MFA - Secure web gateway (explicity proxy) functionality **Hence request to change the specs to below** SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration	Please refer to the revised "Annexure F"
461	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	43	The Proposed solution must provide capabilities to obfuscate sensitive field names in an application to defeat Man-in-The- Browser Attacks on the device itself if required in future via add on licenses	This is specific to a single OEM, hence request to delete the specs	Please refer to the revised "Annexure F"
462	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	79	The SSL Offloader device should have the ability to support C3D	This is specific to a single OEM, hence request to delete the specs	Please be guided by the RFP
463	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	81	The SSL Offloader device should be able to have flexible ICAP request or respond polcies. 1. Enabling ICAP only for HTTP response traffic (It may be useful in some scenarios to only send HTTP response traffic to ICAP, as the vast majority of HTTP GET requests are devoid of payloads.) 2. Enabling ICAP only for HTTP POST request traffic (POST requests will generally always contain a payload, while GET requests usually will not.) 3. Enabling ICAP only for HTTP POST request and all response traffic (This rule will enable ICAP processing on POST requests, all HTTP responses, and would typically be used to filter out normally empty GET and other types of requests.) 4. Enabling ICAP for specific request URL extensions and response content types (Sometimes you just need to activate ICAP for specific file type requests - request URLs that end with something like ".exe", ".sh", or ".bat", and also only scan responses of a specific MIME types (HTTP Content-Type) like "application/json" and application/executable)	**This is specific to a single OEM, hence request to change the specs to below** The SSL Offloader device should be able to have flexible ICAP request or respond polcies.	Please refer to the revised "Annexure F"
464	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	82	The SSL Offloader device should be able to support proxy chaining and act as a explicit forward proxy and following authentication mechanism should be covered 1. Explicit forward proxy authentication 2. Transparent forward proxy authentication (captive portal) 3. Delegate token authentication offload 4. Forward proxy authentication with NTLM 5. Forward proxy authentication with Kerberos	This is specific to a single OEM, hence request to delete the specs	Please be guided by the RFP
465	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	3	Device should be based on dedicated 1U hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 4 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 24 vCPUs scalable to 36 vCPU's.	Query: i. RFP has asked for Less than 2RU i.e. 1RU form factor for Propposed applaiance, which is not true for all OEM, ii. Amount of vCPU asked on same appliance depends on OEM, as every OEM have different way of working, and different size o CPU which changes the need of numbe rof vCPUs and cannot be binding factor and due to this request to relax the specs **Hence we request to relaxy the requriement to below** Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 2 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 16 CPU	Please refer to the revised "Annexure F"
466	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	4	Should have minimum SSL visibility throughput of 115 Gbps from day 1 and scalable to 175 Gbps on same platform with hardware compression.	**Suggestion:** for the SSLo like technology having such high throughput of 146Gbps Scalable to 195G seems to be overkill **Hence request to change the specs to below:** Should have minimum SSL visibility throughput of 120 Gbps from day 1 on same platform with compression capabilities .	Please refer to the revised "Annexure F"
467	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	5	Should support minimum SSL Visiblity TPS: -100 K TPS (RSA 2k keys) from day 1 and scalable to 180 K TPS (RSA 2k Keys) on same platform - 75 K TPS (ECDHE-ECDSA P-256) from day 1 andscalable to 125 K TPS (ECDHE-ECDSA P-256) on same platform	Suggestion: The asked SSL CPS/TPS in the specs seems to be overkill compared to current and future growth and specific to single OEM **Hence request to change the specs to below**: Should support minimum SSL Visiblity TPS: -120 K TPS (RSA 2k keys) from day 1 on same platform - 70 K TPS (ECDHE-ECDSA P-256) from day 1 on same platform	Please be guided by the RFP
468	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR		The SSL Solution should support minimum SSL connections: -L7 requests per second: 4M from day 1 and scalable to 5.5 M on same platform -L4 connections per second: 1.5 M from day 1 andscalable to 2 M on same platform -L4 concurrent connections: 135M from day 1	The Asked specs seems to be specific to single OEM **Hence request to change the specs to below** The SSL Solution should support minimum SSL connections: -L7 requests per second: 4M from day 1 -L4 connections per second: 2M from day 1 -L4 concurrent connections: 135M from day 1	Please be guided by the RFP

469	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	6	The SSL solution should have a minimum of 4x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1	Request to change the specs from 4 100/40G ports to 2 100/40G **Hence request to change the specs to below:** The SSL solution should have a minimum of 2x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1	Please be guided by the RFP
470	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR		The SSL Off loader must have the minimum 24 vCPUs from day 1 and scalable to 36 vCPU's on same platform Memory: 256GB DDR4 Storage: 1 TB SSD	**Suggestion:** Amount of vCPU, Memory and Storage Needed on same appliance depends on OEM, as every OEM have different way of working and cannot be binding factor and **due to this request to relax the specs** **Hence request to relax the specs to below** The SSL Off loader must have the minimum 16 CPU on same platform Memory: 192 GB DDR4 Storage: 500G SSD	Please refer to the revised "Annexure F"
471	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	7	The proposed solution should have a 65 Gbps bulk encryption from Day 1 and scalable to 85 Gbps bulk encryption	**Suggestion:** Having such high SSL throughput for 100Gbps seems to be overkill **Hence request to change the specs to below:** The proposed solution should have a 45 Gbps bulk encryption from Day 1	Please refer to the revised "Annexure F"
472	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	14	The SSL offloader solution must support N+1 and 1+1 inline tool redundancy for inline tools.	Feature asked seems to be clustering which is not desired feature for Network appalince due to unpredicable traffic flow and increses troobleshooting complexity **Hence reques to change the specs to below** The SSL offloader solution must support 1+1 inline tool redundancy for inline tools.	Please refer to the revised "Annexure F"
473	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	18	The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same 1RU rack appliance	Having 1RU form factor seems to be specific to single OEM **Hence request to change the specs to below** The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same appliance	Please refer to the revised "Annexure F"
474	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	39	SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration, Zero trust application access with SAML/Oauth with MFA and Secure web gateway (explicity proxy) functionality with add-on licenses if required in future	**Query:** **The features asked in the specs seems to be specific to perticular OEM and below technology seems not to be related to SSLo Solution** - Zero trust application access with SAML/Oauth with MFA - Secure web gateway (explicity proxy) functionality **Hence request to change the specs to below** SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration	Please refer to the revised "Annexure F"
475	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	43	The Proposed solution must provide capabilities to obfuscate sensitive field names in an application to defeat Man-in-The- Browser Attacks on the device itself if required in future via add on licenses	This is specific to a single OEM, hence request to delete the specs	Please refer to the revised "Annexure F"
476	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	79	The SSL Offloader device should have the ability to support C3D	This is specific to a single OEM, hence request to delete the specs	Please be guided by the RFP
477	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	81	The SSL Offloader device should be able to have flexible ICAP request or respond polcies. 1. Enabling ICAP only for HTTP response traffic (It may be useful in some scenarios to only send HTTP response traffic to ICAP, as the vast majority of HTTP GET requests are devoid of payloads.) 2. Enabling ICAP only for HTTP POST request traffic (POST requests will generally always contain a payload, while GET requests usually will not.) 3. Enabling ICAP only for HTTP POST request and all response traffic (This rule will enable ICAP processing on POST requests, all HTTP responses, and would typically be used to filter out normally empty GET and other types of requests.) 4. Enabling ICAP for specific request URL extensions and response content types (Sometimes you just need to activate ICAP for specific file type requests - request URLs that end with something like ".exe", ".sh", or ".bat", and also only scan responses of a specific MIME types (HTTP Content-Type) like "application/json" and application/executable)	**This is specific to a single OEM, hence request to change the specs to below** The SSL Offloader device should be able to have flexible ICAP request or respond polcies.	Please refer to the revised "Annexure F"
478	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	82	The SSL Offloader device should be able to support proxy chaining and act as a explicit forward proxy and following authentication mechanism should be covered 1. Explicit forward proxy authentication 2. Transparent forward proxy authentication (captive portal) 3. Delegate token authentication offload 4. Forward proxy authentication with NTLM 5. Forward proxy authentication with Kerberos	This is specific to a single OEM, hence request to delete the specs	Please be guided by the RFP
479	Annexure F - Technical Compliance	WAF Technical specs DC-DR	114	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure	**This is specific to a single OEM, hence request to change the specs to below** The solution must have inbuilt/External bypass segments to ensure that fail open in case of hardware failure	Please be guided by the RFP

480	Annexure F - Technical Compliance	WAF Technical specs NDR	114	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure	This is specific to a single OEM, hence request to change the specs to below The solution must have inbuilt/External bypass segments to ensure that fail open in case of hardware failure	Please be guided by the RFP
481		SSL Offloader Tech Specs DC-DR		The solution should support minimum SSL Visibility TPS: - 260 K TPS (RSA 2k keys). | Scalable to 400 K TPS (RSA 2k keys) - 180 K TPS (ECDHE-ECDSA P-256). | Scalable to 300 K TPS (ECDHE-ECDSA P-256) on the same hardware	The RFP has requested 30,000 SSL TPS for the Web Application Firewall, which seems reasonable. The largest payment transactions interface in India has SSL TPS of no more than 50,000. Also, major organizations, like big banks, don't have SSL TPS exceeding 50,000. The SSL TPS requested for SSLO seems excessively high and unrealistic, leading to an oversized requirement. We kindly request you to amend this point **"The solution should support minimum SSL Visibility TPS:** **100 K TPS (RSA 2k keys). | Scalable to 150 K TPS (RSA 2k keys)75 K TPS (ECDHE-ECDSA P-256). | Scalable to 100 K TPS (ECDHE-ECDSA P-256) on the same hardware with license upgrade"**	Please refer to the revised "Annexure F"
482		SSL Offloader Tech Specs DC-DR		Device should be based on dedicated <2U hardware appliance, thishould be dedicated offering from the client and not part ADC Platform. The Platform should have a minimum 4x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 40vCPU scalable to 60 vCPU's	vCPU stands for 'Virtual Central Processing Unit,' denoting a virtualized CPU assigned to a virtual machine (VM) within a virtualized environment. These logical processing units are vital for supplying computational resources to virtualized environments. Notably, virtualization is not a prerequisite for SSL Offloading (SSLO). However, it's worth noting that currently, only one OEM offers a <2U hardware appliance. Additionally, the interface and CPU requirements specified in the RFP are tailored to one OEM, potentially impeding the participation of well-known 'Make in India' OEMs. Therefore, we kindly request modifying this point to: **"Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part ADC Platform. The Platform should have a minimum 2x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 2x32Core processor"**	Please refer to the revised "Annexure F"
483		SSL Offloader Tech Specs NDR		Device should be based on dedicated 1U hardware appliance, this hsould be dedicated offering from the client and not part ADC Platform. The Platform should have a minimum 4x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 24vCPU scalable to 36 vCPU's	vCPU stands for 'Virtual Central Processing Unit,' denoting a virtualized CPU assigned to a virtual machine (VM) within a virtualized environment. These logical processing units are vital for supplying computational resources to virtualized environments. Notably, virtualization is not a prerequisite for SSL Offloading (SSLO). However, it's worth noting that currently, only one OEM offers a 1U hardware appliance with this specifications. Additionally, the interface and CPU requirements specified in the RFP are tailored to one OEM, potentially restrict the participation of well-known 'Make in India' OEMs. Therefore, we kindly request modifying this point to: **"Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part ADC Platform. The Platform should have a minimum 2x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 2x32Core processor"**	Please refer to the revised "Annexure F"
484		SSL Offloader Tech Specs DC-DR		The solution should support minimum SSL connections : - L7 requests per second: 7 M. | Scalable to 10.5 M. - L4 connections per second: 2.8 M. | Scalable to 3.5 M - Maximum L4 concurrent connections: 399 M	For a 50 Gbps SSL throughput, it's possible to expect a range of approximately 10 to 50 million concurrent Layer 4 (L4) Concurrent connections. We request you to change this point to "The solution should support minimum SSL connections : - L7 requests per second: 7 M. | Scalable to 10.5 M. - L4 connections per second: 2.8 M. | Scalable to 3.5 M - **Maximum L4 concurrent connections: 200M"**	Please be guided by the RFP
485		SSL Offloader Tech Specs NDR		The solution should be able to support proxy chaining and act as a explicit forward proxy and following authentication mechanism should be covered 1.Explicit forward proxy authentication 2.Transparent forward proxy authentication 3.Delegate token authentication offload 4.Forward proxy authentication with NTLM 5.Forward proxy authentication with Kerberos	SSLi can integrate with a Forward Proxy solution, where the Authentication mechanism will be handled by the proxy solution. While SSLi can also operate as an explicit proxy, Authentication is not within the scope of SSLi requirements. Therefore, we request that this point be amended to: **"The solution should support proxy chaining and function as an explicit forward proxy"**	Please be guided by the RFP
486		SSL Offloader Tech Specs DC-DR		The solution should be able to support proxy chaining and act as a explicit forward proxy and following authentication mechanism should be covered 1.Explicit forward proxy authentication 2.Transparent forward proxy authentication 3.Delegate token authentication offload 4.Forward proxy authentication with NTLM 5.Forward proxy authentication with Kerberos	SSLi can integrate with a Forward Proxy solution, where the Authentication mechanism will be handled by the proxy solution. While SSLi can also operate as an explicit proxy, Authentication is not within the scope of SSLi requirements. Therefore, we request that this point be amended to: **"The solution should support proxy chaining and function as an explicit forward proxy"**	Please be guided by the RFP
487		SSL Offloader Tech Specs DC-DR		SSL Offloader should support readymade templates for following security devices in service chain 1.checkpoint security Gateway - Layer 2 , Layer 4 & TAP 2. CISCO Firepower Threat Defence - Layer 2 & layer 3 & TAP 3. Fireeye NX inline - Layer 2 & TAP 4. Gigamon inline layer 2 5. Ixia Inline Layer 2 6. PaloAlto NGFW - Layer 3 & TP Layer 2 & TAP 7. CISCO SWA HTTP Proxy 8. Forcepoint SWG HTTP Proxy 9. Fortinet SWG HTTP Proxy 10. Mcfee SWG HTTP Proxy 11. Menlo SWG HTTP Proxy 12. Digital Guardian DLP Via ICAP 13. Mcfee DLP Via ICAP 14. OPSWAT Metadefender Via ICAP 15. SQUID ICAP 16. Symantec DLP ICAP 17. Netscout TAP	SSLO supports integration with all OEMs. While having a ready-made configuration template may be a cosmetic feature lacking in other Make In India OEMs, it shouldn't limit participation. Therefore, we suggest amending this point to: '**The SSL Offloader should support the integration of the following security devices in the security chain.** **1.checkpoint security Gateway - Layer 2 , Layer 4 & TAP** **2. CISCO Firepower Threat Defence - Layer 2 & layer 3 & TAP** **3. Fireeye NX inline - Layer 2 & TAP** **4. Gigamon inline layer 2** **5. Ixia Inline Layer 2** **6. PaloAlto NGFW - Layer 3 & TP Layer 2 & TAP** **7. CISCO SWA HTTP Proxy** **8. Forcepoint SWG HTTP Proxy** **9. Fortinet SWG HTTP Proxy** **10. Mcfee SWG HTTP Proxy** **11. Menlo SWG HTTP Proxy** **12. Digital Guardian DLP Via ICAP** **13. Mcfee DLP Via ICAP** **14. OPSWAT Metadefender Via ICAP** **15. SQUID ICAP** **16. Symantec DLP ICAP** **17. Netscout TAP'**	Please be guided by the RFP
488		SSL Offloader Tech Specs DC-DR		Solution with technical specification and size should be implemented in atleast 3 PSU's/ Private banks/ BFSI in last 3 years in preceding the date of the RFP	We request you to amend this point as it restricts Make in India OEM participation**"Solution with technical specification and size should be implemented in atleast 1 PSU's/ Private banks/ BFSI in last 3 years in preceding the date of the RFP"**	Please be guided by the RFP

#	Section	Ref	Pg/Pt	Clause	Query	Response
489	Section C	Anexxure R	19		Quantity of WAF gateways and Management systems are not mentioned in Annexure R Bill of Quantity	Please refer to the revised "Section E: Scope of Services"
490	Section H	Annexure F, 10		For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authentcated via RADIUS, TACACS+ or via local tabel of authorized users.	Request to modify the clause as "For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authentcated via RADIUS/ TACACS+ / via local table of authorized users."	Please refer to the revised "Annexure F"
491	Section H	Annexure F, 86		The solution must protect system against WASC Wec Security Attack classification.	Request to modify the clasue as "The solution must protect system against WASC Wec Security Attack classification or OWASP top 10."	Please refer to the revised "Annexure F"
492	Annexure F - Technical Compliance	NAC Technical Specificatio n	74	The Proposed Solution must support agent based and Agent less based approach for all the feature & funcationility listed in technical specification/compliance.	The NAC solution should support agentbased and agentless mode to achieve all feature & functionality which includes device visibility , Authentication, classification , Posture accessment , Remediations , Control and Automation, Does our understanding is correct?	Please be guided by the RFP
493	Additional Points			Solution must provide visibility of all IP addressable devices including IP Phone, IP Camera , IP Printers , IP Scanners etc.- IoT (IP Printer , IP Scanner , IP Phone , IP camera etc) Risk Assessment such as -- Detect Unsecure (TCP/UDP port open (For example IP camera having Telnet Port (Port 23) open etc) -- Detect IOT's devices using factory default or Weak/common credentials for SNMP/SSH/TELNET.	Requesting LIC to consider the point since LIC will have ~20% IOT devices which will not support traditional authentication method (such as Radius/Dot1X). It is not a good idea to only depend on 802.1x/MAC address bypass. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. Also MAC address repository should be uptodate at any point in time to meet security aspect.	Please be guided by the RFP
494	Additional Points			Solution must support various controls based on compliance requirement like Move to Quarantine VLAN , ACL, Switch Port block on Wired Network (L2 Switches), It must also support WLAN block, WLAN Role change on Wireless Network (WLC) via IEEE RFC protocols SNMP/SSH and Radius.	NAC solution must support for various blocking option,according to LIC current environment and future request decision will be made during deployment.	Please be guided by the RFP
495	Additional Points			NAC Solution must identify multiple properties change on the endpoint such as application change on the endpoint , Host Name change , OS change , Change in shared folder , User change etc & take the control and notification action automatically based on the LIC security policies.	NAC solution must detect the changes in the endpoints which will helps the LIC to know the actual changes on the endpoint and accordingly LIC can take/modify their compliance for better security.	Please be guided by the RFP
496	Additional Points			NAC solution must support out of box monitoring dashboard for all NAC HW performance parameter like CPU load , Device HDD , Device managed endpoints , Total Memory , Appliance traffic etc	Since in the RFP it is mentioned LIC is providing the HW for NAC deployment , it is important to know the usage/performance of the HW where NAC solution is deployed this dasboard helps the L1/L2 resource to get alert on the resource consumption and take precautionary measure if their is any Indications/abnormalities.	Please be guided by the RFP
497	Additional Points			Proof of Concept (POC) in Live enviroment The LIC at its discretion may ask for the Proof-of-Concept/Value (POC/POV) of the proposed solution in the production set up with the bidders whose bids are technically qualified. 1. The LIC will provide a couple of week's time for conducting POC/ POV at LIC's production environment for the solution proposed in the tender. 2. The LIC may raise certain clarifications during evaluation and the respective bidder should provide the response as per timelines stipulated from time to time without which the bid will be treated as incomplete and may be rejected. 3. Failing to comply with the requirements of the LIC as mentioned in the Tender document or if the solution does not fit into the LIC's production setup due to any third party dependencies etc. then the bid will be treated as incomplete and may be rejected.	Live Proof of Concept (POC) is important for Network Access Control (NAC) projects for several reasons: 1. Validation of Functionality: It allows LIC to validate that the proposed NAC solution works as intended in their specific environment. This ensures that the solution meets the LIC's requirements and effectively addresses the security needs. 2. Identification of Challenges: Live POC helps identify any potential challenges or issues that may arise during deployment or operation. This allows for troubleshooting and fine-tuning before full implementation, minimizing disruptions and optimizing performance. 3. Risk Mitigation: Live POC allows organizations to assess the risks associated with implementing a new NAC solution in LIC environment before committing to a full rollout. This proactive approach helps mitigate potential security vulnerabilities and operational risks. Conducting a live POC for a NAC project helps ensure successful deployment, minimize risks, and optimize the solution to meet the organization's specific requirements.	Please refer to the revised "Technical Bid Evaluation"
498	Annexure F - API Technical Specification				Is there a need for API Manager to provide a multi-tenant solution for different set and owners of APIs using a single deployment and having a centralised portal for managing the same.	API Gateway and Security Solution has been removed from the scope of this RFP
499	Section E - Scope of Services - Sizing Requirements		Pg 70	API Gateway Management and Security - 1000 APIs	What is the overall transaction per second TPS requirement that will need to be supported by the Gateway Component	API Gateway and Security Solution has been removed from the scope of this RFP
500	Annexure F - API Technical Specification		Pt 1	The solution should be an end-to-end API Gateway, Management and Security solution.	Is API Mgmt. Solution, for the API security, expected to be preintegrated & bundled along with Security Solution like SSO, Oauth2, SAML, etc.	API Gateway and Security Solution has been removed from the scope of this RFP
501	Annexure F - API Technical Specification				Does the solution requires flexibility to deploy multiple API gateways as requried & managed using Single Central API Manager at no additional cost of the APIgateway component. This could include internal and External APIs	API Gateway and Security Solution has been removed from the scope of this RFP
502	Section E - Scope of Services - 1. Brief Scope of Work - Support Process Requirement		Pg 61	The support Personnel provided should be conversant with the regular configuration from scratch, integration with other log sources, creation of rules and policies as per LICs requirements, administration tasks, patch management, user management, backup procedures, etc.	Does the solution requries automated upgrade & patching of the components and underlying platform with inplace patch and upgrade management without any downtimes.	Please be guided by the RFP
503	Section E - Scope of Services - 2. Detailed Scope of Work - VII - API Gateway , Management and Security -		Pg 68	The vendor should provide the solution that should allow seamless integration of existing technology/application systems and establish technology platform for future enterprise integrations.	Does the integration platform need to be light weight, modular, with subatomic startup time, with low foorptint reusable extensions and cloud native based on latest techologies like Quarkus with OOTB Connectors and Extension to connect to existing and modern technologies.	API Gateway and Security Solution has been removed from the scope of this RFP

504	Section E - Scope of Services - 7. Service Level Agreements (SLAs) & Penalties		Pg 93	2. Parameter: Uptime Definition: The percentage of time the CASB / NAC / WAF / SSL off loader/MDM/VDI/API Gateway, Management and Security is expected to be operational and available. Target Service Level: 99.99% per month	We Request the LIC to consider a Enterprise Grade Container Orchestration Platform that can be deployed on major Cloud Service Providers and On-prem and Gives flexibility to move the load between these as required, taking advantage of the modern container based technologies that can provide or improve the required Target Service Levels.	Please be guided by the RFP
505	Annexure F - API Technical Specification				Kindly confirm if the proposed solution should support microservices architecture and capable of running as container images, cloud ready.	API Gateway and Security Solution has been removed from the scope of this RFP
506	Section E - Scope of Services - 2. Detailed Scope of Work - VII - API Gateway , Management and Security -		Pg 68	The vendor should provide the solution that should allow seamless integration of existing technology/application systems and establish technology platform for future enterprise integrations.	Does the solution expects the components to be cloud native containerised deployment across Hybrid Cloud on container platform?	API Gateway and Security Solution has been removed from the scope of this RFP
507	Section E - Scope of Services - 2. Detailed Scope of Work - VII - API Gateway , Management and Security -		Pg 68	The vendor should provide the solution that should allow seamless integration of existing technology/application systems and establish technology platform for future enterprise integrations.	Does the solution expects the application/components deployed across Hybrid cloud (Onpremises & Public/Private Cloud) to be managed & secured with single pane of glass	API Gateway and Security Solution has been removed from the scope of this RFP
508	Section E - Scope of Services - 2. Detailed Scope of Work - VII - API Gateway , Management and Security -		Pg 68	24X7 real-time monitoring uptime, availability, health performance of API Gateway, Management and Security devices with mitigation support.	As part of Enterprise Logging & Observability, is it expected functionality to have preintegrated logging & observability functionality as part of underlying platform	API Gateway and Security Solution has been removed from the scope of this RFP
509	Annexure F - API Technical Specification		Pt 28	The Solution should be built to support CI/CD.	Does the solution expect DevSecOps tools to be preintegrated & bundled as part of underlying platform and should not have any additional license/subscription cost to LIC?	API Gateway and Security Solution has been removed from the scope of this RFP
510	Section E - Scope of Services - 1. Brief Scope of Work -On-Site Support Services VII - API Gateway , Management and Security -		Pg 62	The change management of all the devices must be adhering to standards and policies of LIC.	Is there any need for automation tool for installation, patching, configuration mgmt of the components and platforms using a centralised system for all environments including DC, DR, UAT	API Gateway and Security Solution has been removed from the scope of this RFP
511	3. Technical Bid		Pg 22	The bidder must supply a thorough inventory of the hardware components required for the planned implementation of the in-scope solutions. This bill of Quantity (BoQ) as per Annexure R should be itemized separately for all the environments, including DC, UAT and Disaster Recovery (DR).	Are DC, DR and UAT only environments or are there any other environments as well, like Dev, SIT, Pre-Prod, etc.	Please refer to the revised "Section E: Scope of Services" and Revised "Technical Bid"
512	7		17	Responding to this RFP and submission of the bid by the Bidder will be deemed as consent from the Bidder to all the terms and conditions mentioned in this RFP along with its Annexure, clarifications, appendices, addenda, corrigenda issued. The terms and conditions for the bidders who participate in this RFP are specified in the Section named "Terms and Conditions". Responding to this RFP and submission of the bid by the Bidder will be deemed as consent from the Bidder to all the terms and conditions mentioned in this RFP document and the contents of the RFP along with the Annexure(s), clarifications/modifications issued, if any, will be contractually binding on the bidders. All these terms and conditions and the contents of the RFP along with the Annexure(s), clarifications/modifications issued will form the part of the purchase orders/any resulting contracts, to be issued to the successful bidder/s from time to time as an outcome of this RFP Process.	It is submitted that certain terms of the RFP need modification and all such terms may not be discussed during the pre-bid stage. It is hence requested to permit bidders to submit their revisions, suggestions, additions etc. to the terms of the RFP as part of the bid submission. We would kindly request the following edits to be made to the clause: " ~~Responding to this RFP and submission of the bid by the Bidder will be deemed as consent from the Bidder to all the terms and conditions mentioned in this RFP document and the contents of the RFP along with the Annexure(s), clarifications/modifications issued, if any, will be contractually binding on the bidders.~~ **Subject to mutual agreement between the parties,** A all these terms and conditions and the contents of the RFP along with the Annexure(s), clarifications/modifications issued will form the part of the purchase orders/any resulting contracts, to be issued to the successful bidder/s from time to time as an outcome of this RFP Process." We would also request similarly worded language to be amended along the same lines - such as under clause 9 and annexure A.	Please be guided by the RFP
513	15	b	30	Violation of NDA may lead to legal action and blacklisting.	We cannot agree to blacklisting for breach of NDA. Please accept the below modification: "Violation of NDA may lead to legal action ~~and blacklisting~~." We can only agree to this for matters relating to fraud and corrupt practices. We request for the same amendment to be made for clause 21(1)(b) on page 32.	Please be guided by the RFP

#	Section	Sub	Pg	Clause	Query/Request	Response
514	19	g	31	LIC may cancel any procurement under this RFP at any time without assigning any reasons whatsoever. The decision of LIC will be final in this matter.	We would kindly request that the clause be clarified for the following questions: a. can the procurement be cancelled at any point? - e.g after the order has been placed and the vendor has initiated progress on that front b. would all payments for procurements till such date be made? c. would there be a minimum number of days notice required for such cancellation for convenience?	Please be guided by the RFP
515	22		33	In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, or industrial design rights arising from the use of the systems or any parts thereof with relation to the Hardware deliverables, in LIC"s country, the Bidder will act expeditiously to extinguish such claim.	We would kindly request that this be amended in a manner that would reflect that we be liable for permitted uses of the IPR, such as below: "In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, or industrial design rights arising from the *permitted and agreed upon* use of the systems or any parts thereof with relation to the Hardware deliverables, in LIC's country, the Bidder will act expeditiously to extinguish such claim."	Please be guided by the RFP
516	22		34	In no event shall LIC be liable for any indirect, incidental, or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered	We would request that this clause be made mutual to reflect as below: "In no event shall ~~LIC~~ *either party* be liable for any indirect, incidental, or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered."	Please be guided by the RFP
517	24	j	35	The PBG will be invoked in full or part (to be decided by LIC) if the bidder fails to honour expected deliverables or part as per this RFP after issuance of PO during the period of contract. i. The bidder fails to honour expected deliverables or part as per this RFP after issuance of PO. ii. Any legal action is taken against the bidder restricting its operations. iii. Any action taken by statutory, legal or regulatory authorities for any breach or lapses which are directly attributable to the bidder iv. LIC incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.	We request that the clause be amended as below: "The PBG will be invoked in full or part (~~to be decided by LIC~~) *in the eventuality of a material breach* ~~if the bidder fails to honour expected deliverables or part as per this RFP after issuance of PO~~ during the period of contract *and the selected vendor will be provided notice and a cure period of not less than 30 days to rectify such material breaches.* ~~i. The bidder fails to honour expected deliverables or part as per this RFP after issuance of PO.~~ ~~ii. Any legal action is taken against the bidder restricting its operations.~~ ~~iii. Any action taken by statutory, legal or regulatory authorities for any breach or lapses which are directly attributable to the bidder~~ ~~iv. LIC incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.~~ We would kindly submit that the PBG must be invoked only for material breaches and the bidder must be provided a cure period to rectify breaches before PBG is invoked.	Please be guided by the RFP
518	33		37	Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Conditions of Contract Clause, the vendor shall not be liable to LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC; and the aggregate liability of the bidder to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.	We would request that the clause be amended accordingly: "Except in cases of criminal negligence or willful misconduct, ~~and in the case of infringement pursuant to Conditions of Contract Clause,~~ the vendor *neither party* shall ~~not~~ be liable to *the other* ~~LIC~~, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or *business*, interest costs, ~~provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC~~; and the aggregate liability of *both the parties* ~~the bidder to LIC~~, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder ~~provided that this limitation shall not apply to the cost of repairing or replacing defective equipment~~." We cannot agree to indirect and consequential damages for IPR infringement. The exclusion of indirect and consequential damages must also apply to LDs. Limitation of Liability must also apply to costs of repairs and replacements of defective equipment.	Please be guided by the RFP
519	34	a	37	The vendor shall be liable for any delay in execution or failure of their respective obligations under this agreement except for delay caused by occurrence of events beyond control of the vendor, including but not limited to natural calamities, fire, explosions, floods, power shortages, acts of God, hostility, acts of public enemy, wars, riots, strikes, sabotage, order/action, or regulations of government, local or other public authorities.	We would kindly request that this clause be edited as below: "Except for delays caused by occurrence of events beyond the control of the vendor, including but not limited to natural calamities, fire, explosions, floods, power shortages, acts of God, hostility, acts of public enemy, wars, riots, strikes, sabotage, order/action, or regulations of government, local or other public authorities, the vendor shall be liable for any delay in execution or failure of their *previously agreed upon* respective obligations, *beyond the cure period granted* under this agreement. *For clarity - such an event will not preclude LIC from its payment obligations to the vendor*." Please accept new insertion excusing performance in case of Force Majeure situation. LIC's payment obligations not to be covered under such excusing of performance.	Please be guided by the RFP
520	36	A.a	38	Against all actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC.	We request that the clause be amended as below to only include direct claims: "Against all *direct* actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC."	Please be guided by the RFP
521	42	f	41	Recover any dues payable by the selected Vendor from any amount outstanding to the credit of the selected Vendor, including the pending bills and/or invoking PBG or other payment pending from the vendor, if any, under this contract.	We request that the bidder also have a say in this and it is not a unilateral decision.	Please be guided by the RFP
522	47	e	43	LIC may, at any time, by a prior written notice of one week, terminate the successful bidder and / or reduce the scope of the Services	We would kindly request for this time frame to be 30 days as opposed to one week in order to be able to adjust the requirements accordingly.	Please be guided by the RFP
523	Section E	1	50	Please note, the below list of activities is only indicative and not an exhaustive list.	We would kindly request that the list be an exhaustive one so as to account for all the services and costs.	Please be guided by the RFP
524	Section F	1.d.i.	97	LIC may cancel the purchase order placed which will be conveyed to the vendor in writing.	We would kindly request that the clause be clarified for the following questions: a. can the procurement be cancelled at any point? - e.g after the order has been placed and the vendor has initiated progress on that front b. would there be a minimum number of days notice ?	Please be guided by the RFP
525	Section F	1.d.vi.	97	Termination of contract and blacklisting.	We would request that the clause be amended as follows, as we submit that blacklisting should be resorted to only for fraudulent or corrupt practices: "Termination of contract ~~and blacklisting~~."	Please be guided by the RFP

526	Section F	1.e	97	In case of cancellation of orders due to delay in deliveries/installations or deficiency in services etc., besides the penalty being charged, the vendor may also be blacklisted by Life Insurance Corporation of India & may not be allowed to participate in any tenders for a period to be decided by LIC.	We request that blacklisting be restricted to only matters relating to fraud and corrupt practices.	Please be guided by the RFP
527	7		100	The Vendor will indemnify LIC against all third-party claims of infringement of patent, Intellectual Property Rights, trademark, copy right or industrial design rights arising from use of the Vendor „s Solution or any part thereof throughout the Offices of LIC, including but not limited to the legal actions by any third party against LIC. The LIC shall not be held liable for and would be absolved of any responsibility or claim/litigation arising out of the use of any third-party software or its components or modules supplied by the bidder in terms of requirements of this RFP.	We would request that this clause be amended to amended as follows: "The Vendor will indemnify LIC against all **direct** third-party claims of infringement of patent, Intellectual Property Rights, trademark, copy right or industrial design rights arising from **the permitted and agreed upon** use of the Vendor's Solution or any part thereof throughout the Offices of LIC, including but not limited to the legal actions by any third party against LIC. The LIC shall not be held liable for and would be absolved of any responsibility or claim/litigation arising out of the **the permitted and agreed upon** use of any third-party software or its components or modules supplied by the bidder in terms of requirements of this RFP."	Please be guided by the RFP
528	7		100	In no event shall LIC be liable for any indirect, incidental, or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered. For this purpose, it would be immaterial how such liability may arise, provided that the claims against customers, users, and service providers of LIC are considered as a direct claim	We would request that this clause be made mutual.	Please be guided by the RFP
529	8		101	LIC may, at any time, terminate the Contract by giving written notice to the Vendor, if the Vendor becomes bankrupt or otherwise insolvent. In this event, the termination will be without compensation to the Vendor, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to LIC. In case of termination under this clause LIC is liable to pay for all the services performed by the Vendor till the effective date of termination.	We would humbly submit that by going bankrupt or insolvent, it should not preclude us from receiving payments for services that we have already provided and have been accepted. We would request that the clause be amended as follows: "~~LIC~~ **Either party** may, at any time, terminate the Contract by giving written notice to the other party ~~Vendor~~, if the party ~~Vendor~~ becomes bankrupt or otherwise insolvent. ~~In this event, the termination will be without compensation to the Vendor, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to LIC.~~ In case of termination under this clause LIC is liable to pay for all the services performed by the Vendor till the effective date of termination."	Please be guided by the RFP
530	8		102	The following clauses survive the termination and expiry of the contract: a.Intellectual Property Rights. b.Indemnity. c.Insurance. d.Confidentiality and privacy. e.Protection of personal information. f.Security. g.Audit and access h.Knowledge transfer i.Warranty	We would request that other than confidentiality, protection of personal information, knowledge transfer and warranty (the last two subject to the agreed upon period), that the rest be deleted as these are not survival clauses.	Please be guided by the RFP
531	Annexure F - Technical Compliance	CASB Technical Specifications	Excel Sheet -3	The proposed CASB Solution must have at least 5 x Full Compute Edge DC's / POPs / Locations in India to cater DC, DR and NDR scenarios.	The CASB architecture has an edge/PoP architecture where our users get connected tio the nearest edge location wherever the cloud exists to get connected to our PoP , would request LIC to consider this architecture We have currently 2 PoP locations and 4 edge locations	Please refer to the revised "Annexure F"
532	Annexure F - Technical Compliance	CASB Technical Specifications	Excel Sheet -3	The CASB solution must be able to integrate with on-premises AD without any exposure to inbound rules in Firewall from day 1	For on-premise AD integration we require the ADFS interface and for this an inbount access rule from the firewall is required Would request LIC to consider and amend the clause	Please be guided by the RFP
533				The solution must have single light weight user agent <30MB and supported on Windows, MAC, Linux, iOS, Android, shared VDI environments and Chromebooks.	Bidder requests to change this clause to " The solution must have single light weight user agent <30MB and supported on Windows, MAC, Linux"	Please be guided by the RFP
534				The proposed CASB solution must have User Behaviour Analytics (UBA) techniques to analyse user behaviour patterns, detect anomalies, and identify potential insider threats or compromised accounts.	Bidder requests LIC to delete this cluase	Please be guided by the RFP
535				The CASB solution should provide encryption and tokenization mechanisms to protect sensitive data stored in the cloud. This ensures data remains secure even if accessed by unauthorized parties.	Bidder undertanding of the clause is the data in the SSE cloud should be encrypted when stores, hope this understanding is correct	Please be guided by the RFP
536				The proposed solution should have CSA STAR, CIS certifications	We support SOC2 type 2, ISO 27001, GDPR, HIPAA	Please be guided by the RFP
537				The proposed solution must have TrustARC Privacy Certification.	We support SOC2 type 2, ISO 27001, GDPR, HIPAA	Please be guided by the RFP
538				The solution should also support real-time visibility for 50,000+ sanctioned and unsanctioned applications with risk score based on CSA and CSS Standards. The solution should be able to report the security compliances and certifications achieved by these apps	We support 5000+ standard applications, over and above we can incorporate custom applications, we do not support risk scoring of applications as these are standard	Please be guided by the RFP
539				The proposed solution must be able to integrate with Organization IT Corporate Firewalls as well as any existing proxy solution for shadow IT visibility for Risk assessment of traffic from gateway devices in sniff/monitor mode.	Our solution is a standalone SSE solution and does not need to integrate with corporate firewall	Please be guided by the RFP
540				The solution must have Web IPS (Signatures) to protect against targeted user-agent threats.	CASB provides restricted access to application based on configured rules and hence does not need an IPS functionality	Please refer to the revised "Annexure F"
541				The solution must have Web IPS (Signatures) to protect against targeted user-agent threats.	CASB provides restricted access to application based on configured rules and hence does not need an IPS functionality	Please refer to the revised "Annexure F"
542				The solution must be able to add manual IOCs (MD5 and SHA) directly from admin console in real time to minimize risk.	Bidder requests LIC to delete the clause	Please be guided by the RFP
543				The solution must be able inspect & block 5 times zipped / compressed and password protected files.	Bidder requests LIC to delete the clause	Please be guided by the RFP
544				The threat intelligence should be broad and apart from self-intelligence, the OEM should have 40+ Third Party Threat feeds to broaden the threat detection and mitigation landscape	Bidder requests LIC to delete the clause as this clause is too restrictive	Please be guided by the RFP
545				The solution must support 30+ compliance templates including GDPR, PII, PCI, PHI, source code, etc. to ensure necessary compliances.	We support SOC2 type 2, ISO 27001, GDPR, HIPAA	Please be guided by the RFP
546				The solution should support the capability to use new-age technologies like Artificial Intelligence and Machine Learning to understand sensitive documents and images and protect against data leakages over web channel via screenshots, images, and documents.	CASB provides restricted access to application based on configured rules and hence does not need an IPS functionality	Please be guided by the RFP

#	Section	Page	Clause	Bidder Query/Remarks	Response
547				The solution should have capability to provide UEBA profiling and risk score for users based on parameters like data exfiltration, locations awareness, bulk upload and download of files, bulk deletion of files, login-failures etc.	Bidder requests LIC to delete the clause	Please be guided by the RFP
548				The solution should support the capability to enforce user risk scores based access policies	Bidder requests LIC to delete the clause	Please be guided by the RFP
549				The solution must be able to enforce granular activity controls in IaaS Application Category for the Public Cloud Service provider like: Allow, Block, Send, Post, Upload, Download, View, Share, Rename, Move, Invite, Create, Delete, Start, Stop, Reboot, Shutdown, Publish, Preview, Terminate, Register, Reject, Activate, Attach, Login and Logout etc.	We support allow, block, upload and download restrictions	Please be guided by the RFP
550				The solution should have reverse proxy deployment to enforce granular context-specific access policies on unmanaged devices (BYOD) accessing corporate Applications like O365, Google Drive, Gmail etc.	Bidder requests LIC to delete the clause	Please be guided by the RFP
551				The solution should have reverse proxy deployment to enforce granular context-specific access policies on unmanaged devices (BYOD) accessing corporate Applications like O365, Google Drive, Gmail etc.	Bidder requests LIC to delete the clause	Please be guided by the RFP
552				The Solution must have DLP Capabilities and must be able to create DLP Policies based on content, keywords, patterns, exact data matches, size, upload app URLs, user group etc. and a combination of all or some of these.	Bidder requests LIC to delete the clause	Please be guided by the RFP
553				The solution must have inbuilt 2500+ DLP Identifiers.	Bidder requests LIC to delete the clause	Please be guided by the RFP
554				The solution must have inbuilt Incident Workflow Management for DLP Events.	Bidder requests LIC to delete the clause	Please be guided by the RFP
555				The proposed solution must provide Incident Management Console to handle DLP incidents download original file , look at snip of the event, escalate incidents to DLP Incident Manager from the same unified Management Console from day one.	Bidder requests LIC to delete the clause	Please be guided by the RFP
556	Accexure C - Eligibility Criterion	112/113		The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to change to - The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 3 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
557	Accexure C - Eligibility Criterion	112/113		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	request to change to - The bidder during the last 5 years preceding to the date of this RFP should have implemented, and supported the Network Access Control (NAC) OEM to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
558	Accexure C - Eligibility Criterion	112/113		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to change to - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
559	Accexure C - Eligibility Criterion	112/113		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Request to change to -The bidder during the last 5 years preceding to the date of this RFP should have supported the Mobile Device Management (MDM) / OR SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
560	Accexure C - Eligibility Criterion	112/113		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different	Request to change to -The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM / OR API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
561	Accexure C - Eligibility Criterion	112/113		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	EIT will request for this eligibility clause to be removed	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
562	Accexure D - Technical scoring	115/116		Annual turnover during the last 03 (three) years preceding the date of this RFP. ⦿ Greater than INR 500 Crore -> 10 Marks ⦿ Greater than INR 300 Crore up to INR 500 Crores -> 7 Marks ⦿ Greater than INR 100 Crore up to INR 300 Crores -> 5 Marks	Request to change to - Annual turnover during the last 03 (three) years preceding the date of this RFP. ⦿ Greater than INR 1000 Crore -> 10 Marks ⦿ Greater than INR 500 Crore up to INR 1000 Crores -> 7 Marks ⦿ Greater than INR 300 Crore up to INR 500 Crores -> 5 Marks	Please refer to the revised "Annexure D"
563	Accexure D - Technical scoring	115/116		The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. ⦿ Greater than 7 Years -> 10 Marks ⦿ Greater than 5 Years up to 7 Years -> 7 Marks ⦿ Greater than 3 Years up to 5 Years -> 5 Marks	Request to change to -The bidder should have relevant implementation and operational experience ~~for~~ in ~~scope~~ tools to PSU/Government/Private/BFSI Sector ⦿ Greater than 7 Years -> 10 Marks ⦿ Greater than 5 Years up to 7 Years -> 7 Marks ⦿ Greater than 3 Years up to 5 Years -> 5 Marks	Please refer to the revised "Annexure D"
564	Accexure D - Technical scoring	115/116		The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⦿ 2 references of 65000 IP Addresses and above -> 10 Marks ⦿ 2 references of 50000 IP Addresses and above -> 7 Marks ⦿ 2 references of 25000 IP Addresses and above -> 5 Marks	Request to change to -The Bidder during the last 5 years preceding to the date of this RFP, must have supplied OR implemented OR supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms : ⦿ 2 references > 10 Marks ⦿ 1 references> 7 Marks	Please refer to the revised "Annexure D"
565	Accexure D - Technical scoring	115/116		The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⦿ 3 references and above -> 10 Marks ⦿ 2 references and above -> 5 Marks	Request to change to -The Bidder during the last 5 years preceding to the date of this RFP, must have supplied OR implemented OR supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms : ⦿ 3 references and above -> 10 Marks ⦿ 2 references and above -> 5 Marks	Please refer to the revised "Annexure D"
566	Accexure D - Technical scoring	115/116		The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⦿ 3 references and above -> 10 Marks⦿ 2 references and above -> 5 Marks	Request to change to -The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, **OR** implemented OR supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms : ⦿ 3 references and above -> 10 Marks⦿ 2 references and above -> 5 Marks	Please refer to the revised "Annexure D"
567	Accexure D - Technical scoring	115/116		The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⦿ 2 references of 10000 users and above -> 10 Marks ⦿ 2 references of 5000 users and above -> 5 Marks	Request to change to -The Bidder during the last 5 years preceding to the date of this RFP, must have supplied **OR**, implemented OR supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms : ⦿ 1 references of 10000 users and above -> 10 Marks ⦿ 1 references of 5000 users and above -> 5 Marks	Please refer to the revised "Annexure D"

#	Section	Point	Page	RFP Clause	Bidder Query/Request	LIC Response
568	Accexure D - Technical scoring		115/116	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ▢ 4 references -> 10 Marks ▢ 2 references -> 5 Marks	EIT will request that the scoring criteria to be removed	Please refer to the revised "Annexure D"
569	Accexure D - Technical scoring		115/116	The bidder must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ▢ 4 references -> 5 Marks ▢ 2 references -> 2 Marks	EIT will request that the scoring criteria to be removed	Please refer to the revised "Annexure D"
570	Accexure D - Technical scoring		115/116	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ▢ 4 references -> 5 Marks ▢ 2 references -> 2 Marks	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms in India ▢ A Reference having more than 1000 users -> 5 Marks ▢ A Reference having more than 500 users and less than 1000 users -> 2 marks	Please refer to the revised "Annexure D"
571	6. Eligibility Criteria	Point No.04	14	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The Bidder?OEM should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
572	6. Eligibility Criteria	Point No.05	14/15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	We kindly request you to modify the clause as follows: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
573	6. Eligibility Criteria	Point No.06	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
574	6. Eligibility Criteria	Point No.07	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
575	6. Eligibility Criteria	Point No.08	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government /a Private / BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government /a Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
576	6. Eligibility Criteria	Point No.09	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
577	6. Eligibility Criteria	Point No.10	15	The bidder must have a minimum of 15 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / OEM Level Certification. Minimum 3 resources must have OEM Level Certification (preferably of the proposed OEM).	We kindly request you to modify the clause as follows: The bidder must have a minimum of 25 IT Security permanent professionals on their payroll with certifications.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
578	10. Earnest Money Deposit (EMD)	Point No. - i	25	Bidders shall submit along with the bid, EMD of INR 2,00,00,000 (Rupees Two Crores Only) in the form of unconditional and irrevocable Bank Guarantee (BG) as per the format given in Annexure O (Bank Guarantee for E.M.D.). This should be executed by a Nationalized/ Scheduled Bank acceptable to LIC.	We kindly request a reduction in the EMD amount. As a listed entity, we do not qualify for exemption and are required to pay the EMD. Consequently, we must factor this cost into our operations, ultimately leading to an increase in overall expenses. Given that this tender involves an online reverse auction process, it's crucial for us to remain competitive commercially. Therefore, we urge you to consider lowering the EMD amount. This adjustment will encourage more participation from other competitors, enhancing the competitiveness of the tender/RFP process for LIC.	Please be guided by the RFP