CORRIGENDUM - III

[Ref: LIC-CO/IT-BPR/FW/RFP/2023-24/01 Dated : 22/06/2023]					
S.No	**RFP Document Page Number**	**RFP Document Reference(s) (Section & Page Number)**	**Clause (in brief) of RFP requiring clarification(s)**	**Brief details/ Query in reference to the clause**	**Response**
1	32	Section-E: SCOPE OF WORK Details of Work – DDoS solution: Bullet Point 10 page 32	LIC is deploying standalone on Premise DDoS Scrubbing solution with inbuilt Fail Open capability on all of the ports (Copper and Fibre). As per Scope of work this on Premise Inline solution will be deployed in Fail Open Mode to pass through traffic in case if there is any S/w and H/w fault. Bidder should ensure to route the traffic in Always on Mode on the ISP Backbone Scrubber, till the time RMA of the on Premise Scrubber come on LIC DC.	In asked Clause - it mentioned to have Fail Open Mode to pass traffic incise case of Software/ Hardware Fault Internal Bypass is available with only one OEM for asked throughput - This will limit bid to only Single OEM **Hence request to consider External Bypass as well**	Please refer to the revised scope of work
2		Excel: Technical Specs Sheet: On Premise device DC-DR S. No. : 18	The system should be able to work in fail open and fail close mode in all the ports (Copper and Fiber) and should support in-build hardware and software bypass capability	In asked Clause - it mentioned to have Fail Open Mode to pass traffic incise case of Software/ Hardware Fault Internal Bypass is available with only one OEM for asked throughput - This will limit bid to only Single OEM **Hence request to consider below point** The Proposed system must have External Hardware bypass for all interface types	Please refer to the revised-2 technical specifications
3		Excel: Technical Specs Sheet: On Premise device DC-DR S. No. : 61	System should have high perfromance architecture that ensures that attack mitigation does not affect notmal traffic processing and should suport DDoS Flood Attack prevention rate upto 35 Million PPS	For Calculation purpose, if we see complete 30Gbps of traffic with legit - PPS requirement will be 9.6 Million PPS With Clean Pipe service, enabled - no customer will take DDoS attack greater than 5Gbps to 10Gbps on Premise in rise of compromising the setup with 5Gbps of DDoS attack with Minimum Packet Size of 84 Bytes - appliance will need 7.7 Million PPS With 10Gbps of DDoS attack with Minimum packet Size of 84 Bytes - appliance will need 15 Million PPS **So the need for DDoS Flood prevention rate will be in range of 17.3 Million PPS (9.6M - legit + 7.7M - Attack of 5Gbps) ,** **to 24.8 Million PPS (9.6M - legit + 15M - Attack of 10Gbps)** **Hence request to either change the specs to below** System should have high performance architecture that ensures that attack mitigation does not affect normal traffic processing and should support DDoS Flood Attack prevention rate upto 30 Million PPS	Please refer to the revised-2 technical specifications
4		Excel: Technical Specs Sheet: On Premise device DC-DR S. No. : 101	OEM Anti-DDoS Solution should be deployed and used by at least 4 Tier 1 (class A) Internet Service Provider (ISPs) in India to protect their own Core infrastructure or offer Clean Pipe Service from DDoS Attacks	Only 1 OEM have 4 Tier 1 ISP presence in India, and this will limit the bid to single OEM **Request to change the ask of At Least 4 Tier 1 ISP to 2 Tier 1 ISP and change the specs to below:** OEM Anti-DDOS Solution should be deployed and used by at least 2 Tier 1 (class A) Internet Service Provider (ISPs) in India to protect their own Core infrastructure or offer Clean Pipe Service from DDoS Attacks	Please refer to the revised-2 technical specifications
5		Excel: Technical Specs Sheet: On Premise device NDR S. No. : 18	The system should be able to work in fail open and fail close mode in all the ports (Copper and Fiber) and should support in-build hardware and software bypass capability	In asked Clause - it mentioned to have Fail Open Mode to pass traffic incise case of Software/ Hardware Fault Internal Bypass is available with only one OEM for asked throughput - This will limit bid to only Single OEM **Hence request to consider below point** The Proposed system must have External Hardware bypass for all interface types	Please refer to the revised-2 technical specifications

6		Excel: Technical Specs Sheet: On Premise device NDR S. No. : 61	System should have high perfromance architecture that ensures that attack mitigation does not affect notmal traffic processing and should suport DDoS Flood Attack prevention rate upto 35 Million PPS	For Calculation purpose, if we see complete 30Gbps of traffic with legit - PPS requirement will be 9.6 Million PPS With Clean Pipe service, enabled - no customer will take DDoS attack greater than 5Gbps to 10Gbps on Premise in rise of compromising the setup with 5Gbps of DDoS attack with Minimum Packet Size of 84 Bytes - appliance will need 7.7 Million PPS With 10Gbps of DDoS attack with Minimum packet Size of 84 Bytes - appliance will need 15 Million PPS **So the need for DDoS Flood prevention rate will be in range of 17.3 Million PPS (9.6M - legit + 7.7M - Attack of 5Gbps) ,** **to 24.8 Million PPS (9.6M - legit + 15M - Attack of 10Gbps)** **Hence request to either change the specs to below** System should have high performance architecture that ensures that attack mitigation does not affect normal traffic processing and should support DDoS Flood Attack prevention rate upto 30 Million PPS	Please refer to the revised-2 technical specifications
7		Excel: Technical Specs Sheet: On Premise device DC-DR S. No. : 101	OEM Anti-DDoS Solution should be deployed and used by at least 4 Tier 1 (class A) Internet Service Provider (ISPs) in India to protect their own Core infrastructure or offer Clean Pipe Service from DDoS Attacks	Only 1 OEM have 4 Tier 1 ISP presence in India, and this will limit the bid to single OEM **Request to change the ask of At Least 4 Tier 1 ISP to 2 Tier 1 ISP and change the specs to below:** OEM Anti-DDOS Solution should be deployed and used by at least 2 Tier 1 (class A) Internet Service Provider (ISPs) in India to protect their own Core infrastructure or offer Clean Pipe Service from DDoS Attacks	Please refer to the revised-2 technical specifications