Section-E: SCOPE OF WORK

The scope of work includes understanding the requirement, customizing and providing the deployment architecture of proposed solution. Supply, install and commission the respective links along with appliances at LIC data centers. Configure the links and appliances, tune up the appliances with LIC Security requirement; document the solution, Train & Certify candidates nominated by LIC. This is not an all-inclusive list. The Bidder is expected to provide the end to end solution and bidder is expected to absorb any other cost of material / services if any not particularly listed below.

The proposed solution should seamlessly integrate with existing network/security setup of LIC without requiring purchase of additional equipment/components/Software etc. It should also seamlessly integrate with any future standard procurement made by LIC without requirement of downgrading or upgrading of existing equipment/ components / software used by LIC. However, if any additional equipment/components/Software etc. is required for seamless integrate with existing network/security setup of LIC; the same has to be provided at no additional cost to LIC.

The successful bidder must provide all necessary hardware for supporting the requirements laid down in this RFP (including the technical specifications) from day one with full hardware warranty and support for the complete contract duration. Bidders must include all required compute, storage, OS, database license and any other software licenses required for the solution to work

General
- Commissioning of links and Supply of on-premise DDoS device/appliance with provision for version upgrades / patches.
- Commissioning of links, installation and implementation of the products/devices as per the security architecture design.
- Vendor has to act as technical-advisor to LIC for DDoS related security threats by way of evaluation, demonstration, etc. as and when required by LIC. Vendor has to submit findings/reports to LIC and give suggestions/recommendations. Necessary resources (including Level-3 support) have to be deployed by vendor for technical assistance and submit the detailed documentations etc. No additional cost will be payable by LIC for such things.
- Identifies potential security risks, helping LIC to take appropriate, corrective action.
- Design, implement, and keep record & controls and migration to IPv6 as and when required by LIC without any additional cost to LIC.
- In case there is a cost incurred to LIC due the wrong BoM/Specification/feature-set of security equipment/device/appliance at any location, the same will have to be replaced by vendor at no extra cost to LIC.
- Prepare test-plan, migration plan and rollback strategies.
- Monitoring and offsite support.
- The successful bidder shall co-ordinate and co-operate with the other vendors appointed by the LIC, if required so that the work shall proceed smoothly without any delay and to the satisfaction of LIC.
- No extra claim shall be entertained on account of all/part of any job redone on account of bidder's negligence which results into damages/losses during execution of the job. Also, any component(s) required to deliver the solution after release of Purchase Order shall have to be provided by the successful bidder. All such cost shall be borne by the bidder.
- The vendor has to provide complete escalation matrix which should be updated and sent to LIC as and when there is a change.
- The Bidder has to perform OEM audit of the deployment, once the commissioning is over, and provide a detailed report on the entire deployment including verification of the various technical aspects as per the requirements of RFP, hardening and best practices that have been adopted. Remediation action to the OEM report has to be undertaken by the bidder.

Design and Architecture:

- Total solution will cover commissioning, installation of on-premise device, implementation, integration of on-premise device with the cloud/scrubbing center, testing, training, reporting etc.
- Bidder needs to study existing LAN & WAN network environment of LIC and design the solution accordingly.
- Prepare HLD and LLD in consultation with OEM and LIC for implementation. The design should be OEM certified.
- Detailed Network Connectivity Diagram (including last mile connectivity, firewall etc.) for the proposed solution is to be provided by the bidder.
- Design and document a Project implementation plan with significant milestones marked on it.
- Prepare the designs and implement the solution in line with existing regulatory guidelines as modified from time to time.
- Bidder needs to prepare a detailed execution plan. The complete documented plan must be submitted to LIC with supported designs and drawings (if any) within 2 weeks of placing the order. The actual execution will start only after approval of plan by LIC officials.
- The plan shall include information related to required downtime, deployment schedule etc. The commissioning of links and installation of the devices shall be done as a planned activity on a date & time of approved deployment schedule.
- The successful bidder need to install all the associated equipments needed to complete the job as per the specification described in this tender.
- The commissioning of links shall include end to end commissioning of the links by the service provider as mentioned in the RFP.
- The commissioning/installation will include proper mounting, labeling, tagging of all equipment and provide network and power connections.
- The bidder shall be responsible to provide within scope of work all facilities like labor, transportation, tool Kits, testing equipment etc. which is necessary for successful deployment of solution.
- Transportation to & fro, lodging and boarding of manpower shall be in vendors scope.

Details of Work – Link commissioning and maintenance:

- Commission two 500Mbps and two 100 Mbps dedicated (1:1; uncompressed, unfiltered and unshared) Premium Internet Bandwidth with dual last mile (for redundancy).
- The ISP shall provide dual last mile (from two different service providers)
- It is the responsibility of vendor to factor in all related infrastructure required to commission the links, including cable, connectors etc. They should not depend on LIC for any provisioning in this regard except router and switches.
- This link shall be terminated on DDoS device.
- The router /switch which will be arranged by the LIC at the Data Centers. Presently the links are terminated on switch and LIC is using Cisco ASR1002-HX router. However, LIC may change the router in future.
- The link may be terminated on Ethernet or on the Fiber port of the router. The bidder has to make provisions for both.
- LIC will provide access to the router for commissioning of links and making configurations for proactive monitoring of the links.
- The winning bidder shall provide /24 Public IP addresses (IPv4) and /48 Public IP addresses (IPv6) for the 500 Mbps links. For 100 Mbps links the winning bidder shall provide /28 Public IP addresses (IPv4) and /24 Public IP addresses (IPv6)
- LIC may, however, make arrangements for Public IP Addresses and ASN from the APNIC. In that case and on demand from the LIC, the successful bidder shall unconditionally have to configure these IP addresses and on successful commissioning, will withdraw their own IP addresses.
- If there is any reduction in the charges related to ports, bandwidth etc. due to changes in Government Policy etc., the benefit of subsequent price reduction shall be passed to LIC. LIC reserves the right to re-negotiate the charges based on market conditions after each year of completion within the contract period apart from any other reductions in tariffs due to Government policies etc.
- The Internet leased links should adhere to the specifications mentioned in technical specifications (links) mentioned in the RFP.
- The ILL Setup should be easily scalable.

> The bidder has to factor in the cost of shifting of links and the DDoS device, at least once during the entire contract period for each location.

Link Maintenance:
> The vendor has to monitor the link proactively on a real time basis. LIC will provide access to the router for making configurations for proactive monitoring of the links.

> Bidder shall maintain the connectivity on 24*7*365 basis and shall rectify the defect by pro-active monitoring so as to maintain the Service Level Agreement

> Complaint shall be lodged preferably over web portal, but other modes such as email etc. with the designated officials of the bidder, should also be available.

> The bidder shall provide a dedicated portal/web interface/site for LIC for logging calls (trouble tickets), viewing status of calls (trouble tickets), escalation of trouble tickets, monitoring the status of links, monitoring performance parameters of links such as periodical downtime etc.

> The portal/web interface/site shall provide reports regarding the above as and when required by LIC. In addition the successful bidder shall provide Out-of-the-box reports and customized reports templates based on the needs of LIC (based on mutual discussion).

> The bidder shall issue a unique number identifying the complaint lodged by LIC.

> During the tenure of the contract or till link is being used at the site, the bidders shall bear all the operational costs associated with link commissioned.

> Bidder has to submit details of International Gateways (No. Of Gateways, Name of Gateway, Location of Gateway, Own or Not etc.).

> Details about bidders POP from which last mile will be extended to LIC's various centers.

- Location of the POP (please give full details)
- Nearest POP to LIC with distance
- Details of last mile connectivity with Type of the connectivity, ownership (own/third party etc.).

> Bidder has to submit escalation matrix and keep it up to date during the entire period of the contract.

> The selected bidder shall be responsible for the preparation of "Change Management Process" document for the LIC wherein the entire process/procedure shall be defined pertaining to various activities involved during the tenure of the contract.

> Notwithstanding anything mentioned above, LIC reserves the right to reject the contract or cancel the entire process, with 30 days' notice, without assigning reasons thereto.

> The bidder shall arrange and ensure proper contingency plans to meet any unexpected obstruction to the Service Provider or any employees or sub-contractors of the Service Provider (as LIC may permit) in rendering the Services or any part of the same under this Agreement to LIC.

Continuity

> The bidder agrees for the following continuity arrangements to ensure the business continuity of LIC:
> In the event this Agreement comes to end on account of termination or by the expiry of the term/ renewed term of the Agreement or otherwise, the Service Provider shall render all reasonable assistance and help to LIC and to any new contractor engaged by LIC, for the smooth switch over and continuity of the Services.

> In the event of failure of the Service Provider to render the Service, without prejudice to any other right LIC shall have as per this Agreement, LIC at its sole discretion may make alternative arrangements for getting the Services from any other source. And if LIC gives a prior notice to the Service Provider before availing such service from any other alternative source, the Service Provider shall be liable to reimburse the expenses, if any incurred by LIC in availing such services from the alternative source.

Details of Work – DDoS solution:

> The DDoS solution should be Hybrid in Nature with On-Premise device with Cloud Signaling to Scrubbing Center.
> The on-premise device provided by the bidder should be able to provide protection against all types of DDoS attacks, for all the existing and future links procured at by LIC at the data centers in which they are

deployed. Once LIC, makes arrangements for Public IP Addresses and ASN from the APNIC, the successful bidder shall unconditionally have to protect all links from volumetric attacks also in future.

- LIC may, however, make arrangements for Public IP Addresses and ASN from the APNIC. In that case and on demand from the LIC, the successful bidder shall unconditionally have to protect all links from volumetric attacks in future.
- The various types of attacks that should be mitigated for all the links, mentioned in the point above, are provided in technical specifications.
- The ISP shall provide comprehensive DDoS attack detection and protection facility to LIC and filter the traffic as per LICs requirement
- Providing complete solution including hardware, software, service, updates and other required components; supply, deployment and implementation, integration, and configuration of Anti DDoS cloud and On-Premise solution.
- Seamless integration of on-premise device with the scrubbing center.
- All appliances must have inbuilt hardware and software bypass functionality to continue business operations in case of failures.
- LIC is deploying standalone on Premise DDoS Scrubbing solution with inbuilt/external 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.
- The on-premise DDoS appliance should support the DDoS mitigation as per the technical specifications mentioned in the RFP.
- The proposed service must cover volumetric attack mitigation which can mitigate attack of any size.
- The On-Premise solution to adhere to the technical specifications mentioned in technical specifications sheets.
- The Scrubbing Centre and the cloud solution should adhere to the technical specifications mentioned in technical specifications sheets.
- The bidder will provide telephonic & offsite / onsite support during complex DDoS attack event, if LIC needs assistance, without extra charges. The support would include assistance for attack mitigation, providing assistance for Zero-day DDoS Attacks, fine tuning the appliances if required, trace-back and reports generation etc.
- The bidder should also work on the backend with OEM TAC/ SOC for faster resolution of the DDoS threat.
- In case of any incident, bidder should identify the attack vectors, the root cause of the attack & suggest preventive measures to avoid facing similar type of attacks again.
- The Solution should have comprehensive support for a period of 5 years, as and when required, from the date of acceptance given to the Bidder.
- The Bidder should provide backup solution for proposed setup. The backup taken should be SHA-256 encrypted.
- The equipment quoted by bidder should not be declared as End of Sale by the OEM at the time of project implementation Signoff. The product should not be end of support for next 6 years.
- The solution proposed should be integrated seamlessly with the systems like SIEM, SOAR, NMS etc. The vendor will be responsible for integration of the same.
- Solution should also integrate with the email for alert information flow.
- The Bidder must specify all hardware specifications in detail. The Bidder needs to mention about the communication media (Copper Wire or Fiber) being used.
- The bidder needs to provide training to 5 LIC officials by OEM certified trainer in Mumbai, within three months of installation.(at LICs premises)

Basic Installation of Hardware and Software

Bidder has to perform following jobs for completing the above mentioned activity:
- Mounting physical devices onto racks as required.
- Powering on the physical devices & running Hardware Diagnostics.
- Installing the required OS and Applications on Physical Hardware.
- Configuring IP address and default gateway etc. on all devices

- ➢ Check L2 & L3 connectivity on network using "ping & trace route" commands
- ➢ Installing License on the appliances.
- ➢ Enabling of features and functionality on the appliances as per details mentioned in the technical specification etc.
- ➢ Configure all automated updates for all security features.
- ➢ Configuration of update and upgrades as and when the latest version is released.
- ➢ Configuring backup Schedule of appliance, Management, Logging and Reporting appliance.
- ➢ Check for Fail open between appliances.
- ➢ Quarterly DDoS life cycle review in the form of executive summary report providing DDoS threat landscape in LIC.
- ➢ Review of potential threats and reconfiguring the system as per requirements.
- ➢ Setting up basic system health monitoring and log analysis.

Reporting and Governance

Reporting would involve the tasks listed below. The list is not exhaustive but only indicative. The reporting requirements may further evolve and the bidder has to absorb any other cost while quoting for the bids .

- ➢ Creating Out-of-the-box reports and customized reports templates based on the needs of LIC.
- ➢ Near time reporting dashboard: - Integrated dashboard where the operations can be viewed and can be drilled down to the further details. This should be near real time view as per requirement where the dashboard should display latest information.
- ➢ Dashboard for governance: - Governance dashboard means a dashboard for viewing all governance related KPI's, progress, action, status etc. for security and compliance related KPI's.
- ➢ TCP dump report when under DDoS attack for forensic analysis
- ➢ Granular logging policy per application
- ➢ Acting on SOC,CERT-IN threat intelligence and alerts and taking preventive measures
- ➢ Assist in preparation of reports for LIC, to be submitted to regulatory bodies as and when required with respect to DDoS.
- ➢ Provide reports as mentioned under the reporting section of the technical specification.

Continuity–DDoS

- ➢ The bidder agrees for the following continuity arrangements to ensure the business continuity of LIC:

- ➢ In the event this Agreement comes to end on account of termination or by the expiry of the term/ renewed term of the Agreement or otherwise, the Service Provider shall render all reasonable assistance and help to LIC and to any new contractor engaged by LIC, for the smooth switch over and continuity of the Services.

- ➢ In the event of failure of the Service Provider to render the Service, without prejudice to any other right LIC shall have as per this Agreement, LIC at its sole discretion may make alternative arrangements for getting the Services from any other source. And if LIC gives a prior notice to the Service Provider before availing such service from any other alternative source, the Service Provider shall be liable to reimburse the expenses, if any incurred by LIC in availing such services from the alternative source.

Documentation
- ➢ All the documents shall be supplied in properly bound volumes of A4 size sheets.
- ➢ Three sets of hardcopies as applicable and one softcopy on CD/USB Storage shall be supplied as final document.
- ➢ Documents for high level design, detailed design, configuration of individual features set on various appliances, general testing, scenario based fail-open testing, Standard Operating Procedure in accordance with the IRDAI guidelines (exhaustive including backup, Procedures, Quality Assurance/Quality Control etc.), best practices etc. shall form the complete set for fulfilling the documentation criteria.

- The SOPs have to be reviewed quarterly and changes, if any, have to be incorporated. In either case (with changes or without changes) the updated version of SOP in the latest quarter has to be prepared and submitted.
- Vendor shall also submit Delivery and Installation Report, Warranty certificates, License Copies for all the items supplied along with the supplies.
- Installation report should contain the part numbers of all the components supplied by the selected bidders.

Acceptance by LIC

- The Goods supplied by the Bidder should meet the technical specifications envisaged in this tender document.
- A comprehensive "Acceptance Test Plan" document, containing various aspects of the 'Acceptance Test' to demonstrate all the features of the proposed Solution, shall be submitted by the bidder.
- Scenario based Acceptance Test shall be carried out jointly by the representatives of LIC and the Bidder after the Installation.
- Acceptance tests should explicitly demonstrate provision of the Links, commissioning, testing, fine tuning of the links, Integration with LIC Network, DNS ,testing the input & output errors of the links, testing of the bandwidth, testing of latency, Packet Delivery, Packet drop , jitter, High Availability (HA) features, dual last mile feature, automatic failover features, desired DDoS features etc.
- Appliances will be considered to have been commissioned when all services as described in this tender document are able to run smoothly over the network. Mere installation of appliances with out-of-the box features will not constitute as commissioning of the proposed solution.
- The final acceptance will be provided by LIC after verifying all aspects as mentioned in the document have been delivered to satisfaction.

LIC has the right to the following aspects:
- Access Control (logical, physical, administrative etc.) of all appliances has to be shared with LIC officials, but vendor should implement in such a way that accountability can be fixed,
- The vendor will do the necessary changes in the infrastructure as per the changing business needs without charging any cost to LIC.

Performance and Support Assurance

The System Integrator and OEM must provide the following performance assurances on the DDoS solution:

- During the immediate post deployment demonstration of the DDoS mitigation solution in the live environment, the system integrator and OEM must demonstrate that the Memory and CPU utilization of the equipment doesn't exceed 35% of the total memory and CPU capacity. In case this requirement is not met, then the OEM and System Integrator must replace the equipment with a higher capacity box to meet this requirement without any additional cost implication to the LIC.
- The OEM and System Integrator must assure that all types of support including warranty, security, upgrade and maintenance support for hardware, software and any other component shall be available throughout the contract period. In case any of the components of the solution is declared end of support by the OEM, the same shall be replaced with an equivalent or higher component without any cost implication to the LIC. Solution/upgrade for any newly emerged threat/vulnerabilities must be provided without any additional cost to LIC.
- Stage of Product life cycle: The Software and engineering support for all the equipment/devices offered in the Total Solution must be available till the end of Contract Period (Taking into account the implementation period from the date of purchase order). During SW and Engineering support the OEMs would continue to develop, repair, maintain, and test the product software including operating system and release appropriate bug-fixes/patches/updates. Documentary evidence for "Stage of product Life Cycle" must be from the information/documents available in public domain.

The solution must be able to provide reporting and MIS as per the detailed specifications. In case, OEM is not able to provide the same, third party software/hardware may be used. For any such third-party tool and/or tool of the OEM/s the respective OEM of the DDoS equipment will be responsible and accountable for smooth, efficient and

effective performance of such tools during the entire contract period

RACI Matrix

Below Table depicts desired RACI (Responsible-R, Accountable-A, Consulted-C, Informed-I) matrix for proposed engagement which is non-exhaustive. The successful bidder must submit comprehensive RACI for proposed services in a similar way in their response to RFP.

Activity	SI	OEM	LIC
Plan, Design, Implementation	R,A, Implementation	R,A	C, I
Device Monitoring Best Practices Audit- Identify existing monitoring parameters, recommended monitoring practices, and formulate a corrective action plan.	A	R	C,I
Device and Performance Monitoring	R,A	C	I
Monitoring Tool/Software availability and Support	R,A	R,A	C, I
Service Request Handling	**R,A**	**C**	**I**
Incident Detection and Notification	R,A	C	I
Incident Troubleshooting	A	R	C,I
Incident Communication Updates	R,A	R,A	C,I
Incident Escalation	R,A	R,A	C,I
Incident Closure- Restoration	R,A	R,A	C,I
Problem Management- Root Cause Analysis (24 hours)	R,A	R,A	C,I
Configuration Change Plan	R,A	C	I
Impact Analysis and Change Validation	R,C	R,A	I
Change Approval	A	C,I	R
Change- Method of Procedure	R	A	C,I
Change Execution	R,A	A	C,I
Change Communication	R,A	C	I
Third Party and/or OEM's own additional tool for DDoS management and performance analysis	R,A	R,A	C,I
Proactive Software Risk Assessment/ Software Selection	R,C	R,A	I
Software Implementation	R	A	C,I
Software Security Vulnerability Assessment	R	A	C,I
Configuration Audit, Best Practices	R,A	R,A	C,I
Configuration Remediation	R,A	C	I
Capacity Audit and Benchmarking	A	R	C,I
Performance Audit	R,A	R	C,I
Capacity and Performance Monitoring	R,A	C	I
Inventory Management	R,A	C	I

License Management	R,A	C	I
Reporting	R,A	C	I
SLA Performance	R,A	R,A	C,I
SLA Reporting	R,A	C	I
Service Delivery Review and Governance	R,A	R,A	C,I
First Information report (FIR) on incident (1 Hour)	R,A	R,A	C,I
Business Continuity Management	R,A	R,A	C,I
Proactive Threat Assessment	R,A	R,A	C,I

Service-Delivery and Project Management

The project manager/SDM may be shared resource, but he/she has to act as the Single Point of Contact for LIC for all aspects related to the project. The onsite SDM should have the following minimum profile:
   a) Minimum 2 years of experience in the domain of ILL and DDoS
   b) Must aware and having knowledge of Service Delivery processes.
   c) Experience of handling/managing teams (Minimum 5 reportees).

The responsibilities of the On-site Service-Delivery Manager as a part of support are as follows *(indicative but not exhaustive):*
   a) Act as a Single Point of Contact (SPOC) for the entire project
   b) Responsibility for the entire execution & management of the project after receipt of purchase order. (ii) Overall monitoring of project
   c) Co-ordination for Delivery/Installation of New hardware in stipulated time frame
   d) Call flow management, Quality Service Delivery
   e) Overall monitoring and management of network gateway security and related services
   f) SLA management and reporting
   g) Submission of periodical Reviews and reports required by LIC.
   h) Crisis management and Emergency response procedures.
   i) Preparation and submission of detailed Project documentation to LIC (Purchase Order wise) and progress of initiatives taken by LIC.
   j) He should be placed at LIC premises during LIC's office hours. However, the hours may be extended whenever required.

The Vendor shall submit to ED (IT/BPR), CO, Mumbai the name and contact details, including address, telephone number, mobile number, FAX number/email address of the nominated Service-Delivery Manager.

It is mandatory for the concerned Service-Delivery Manager to have structured meeting with the ED(IT/BPR)/Secretary(IT)/Dy. Secretary(IT)/Assistant Secretary (IT), Security Section of Central Office once a week, preferably on Monday, during the implementation period from the date of receipt of the first Purchase Order by the vendor. Weekly meetings should be held till the project is entirely rolled out.

In short, Onsite Service-Delivery Manager shall carry out and coordinate the various tasks involved in the project like Project scheduling, tracking, monitoring, identifying risks, liasioning with all stake holders *(OEM, vendors' back-end teams etc.)* and reporting to LIC on the overall progress of the project, etc. No charges will be payable by LIC for the onsite Service-Delivery Manager.

Remote (offsite) Support

The successful Bidder has to provide throughout the contract period, the services of 24x7 offsite support stationed at Mumbai and Bengaluru. The roles and responsibilities of offsite support would be to provide end to end support for

the deployed solution. She/he will have to visit LIC's premises as and when required. The intimation regarding his/her presence onsite will be sent through mail/telephonic call/Text message/Whatsapp message. The offsite support has to report at LICs premises within two hours of the receipt of request from LIC's designated official. There might be instances where the requirement would be beyond office hours or on holidays and Sundays. Even in such eventualities the offsite support has to report at LICs premises within the stipulated time period of two hours.

 In addition he has to alert/escalate LIC officials (as per matrix provided) in the event of any security threat.
The offsite support has to be provided within 8 weeks of issue of PO. The details of offsite support such as name, Contact no., email ID etc. has to be provided to LIC within the same time period. The complete escalation matrix for offsite support has to be provided to LIC within 8 weeks. The offsite support has to monitor the setup remotely. VPN connectivity, if required, shall be provided by LIC.