प्रगत संगणन विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

PRE BID QUERIES CLARIFICATIONS for Bid No. GEM/2024/B/4508521

The queries received during the Pre-Bid meeting held on 24.01.2024 from various prospective bidders were consolidated and clarifications are provided in the C-DAC Response column of the Table.

* Bidders are here by notified the following

1. Due date for submission of bids will not be extended under any cricumstance due the Project Commitments.
2. As CDAC does not qualify for any GST Rebate or Concession. Hence Bidder need to quoted as per the applicable GST.
3. The Licenses for Software/Tools shall be perpetual, bidder shall take the same into consideration while submitting the bid.
4. All the incidental expenditure inccured towards replacement of the faulty spares has to be borne by the supplier.

SN	BoQ Item	Tender Ref	Tender Specs	Change Requested	C-DAC Response
1	(i) Server / HCI	2. RAM	Minimum 1.5 TB DDR5 RAM (expandable up to 3 TB without replacing the supplied modules)	Minimum 1.5 TB DDR5 RAM (expandable up to 3 TB)	No Change. (Expected to supply with 128 GB RAM modules)
2	(i) Server / HCI	6. Remote Management	1. 1 Gbps iLO Management port	1 Gbps iLO/iDRAC Management port 1 Gbps out of band management port	May be read as follows: 1 Gbps BaseT Ethernet port for out of band, web based remote management of the server with features to monitor the health of the servers through web & SNMP, view the physical inventory of server and reset power / reboot server.
3	(i) Server / HCI	7. OS Certifications	Certifications from major Hypervisor OEMs – VMWare and Nutanix and certified for proposed cloud solution and softwrae defined storage solution.	Certifications from major Hypervisor OEMs – VMWare or Nutanix	May be read as follows: Certifications from major Hypervisor OEMs – VMWare / Nutanix and certified for proposed cloud solution and softwrae defined storage solution.
4	(i) Server / HCI	4. HDD	2. RAID 1, 5 supported by RAID Controller with 2 GB Cache 1 x 800 GB SSD Cache drive minimum endurance of 3 DWPD for 5 years	Remove the clause	No Change
5	(i) Server / HCI	5. HBA	2 x Single port 32 Gbps HBA Cards	Remove the clause	No Change

6	(ii) Cloud Management Software	2. Compute Virtualization 1.0	1. Virtualization layer should sit directly on the bare metal server with features like HA, Proactive HA, Zero Downtime & Zero Data-loss without any additional clustering solution, Encrypted Live Migration of VMs, Hot Add (vCPU, vMemory, vStorage & vNetwork) without disruption or downtime of working VMs for both windows & Linux based VMs, distributed switch, VM level encryption, Network & Storage I/O Control, VM based replication with min. 5mins RPO, predictive dynamic resource scheduling for storage and VMs, secure the VMs with offloaded AV/AM, HIPS/ HIDS and stateful firewall solutions without the need for agents inside the VMs of windows & Linux.	Request you to change it as - 1. Virtualization layer should sit directly on the bare metal server with features like HA, Zero Downtime & Zero Dataloss without any additional clustering solution, Encrypted Live Migration of VMs, Hot Add (vCPU, vMemory, vStorage & vNetwork) without disruption or downtime of working VMs for both windows & Linux based VMs, distributed switch, VM level encryption, Network & Storage I/O Control, VM based replication with min. 5mins RPO, predictive dynamic resource scheduling/hot-spot contention resolution for storage and VMs, secure the VMs with offloaded AV/AM, HIPS/ HIDS and stateful firewall solutions without the need for agents inside the VMs of windows & Linux. ------- We hereby understands that IDS and IPS solution has already been running at networking hardware perimeter label in CDAC Hyderabad / Noida site. Kindly confirm Y/N As per RFP, you have asked “VMs, secure the VMs with offloaded AV/AM, HIPS/ HIDS and stateful firewall solutions without the need for agents inside the VMs of windows & Linux” We recommend to remove this clause if IDP/IPS solution is already running at perimeter hardware. Furthermore, HIPS / HIDS adds operational complexity to configure this use case and system overhead with network traffics monitoring in HCI architecture. Hence, requesting to modify this clause as per following. "Virtualization layer should sit directly on the bare metal server with features like HA, Proactive HA, Zero Downtime & Zero Dataloss without any additional clustering solution, Encrypted Live Migration of VMs, Hot Add (vCPU, vMemory, vStorage & vNetwork) without disruption or downtime of working VMs for both windows & Linux based VMs, distributed switch, VM level encryption, Network & Storage I/O Control, VM based replication with	No Change. If proposed solution do not have requested features, can integrate 3rd party virtual appliances in order to achieve functionalities.
7	(ii) Cloud Management Software	2. Compute Virtualization 2.0	2. The solution should provide proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.	2.The solution should provide High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.	No Change
8	(ii) Cloud Management Software	2. Compute Virtualization 5.0	5. The solution should provide in-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details	Request you to eloaborate these points in pre-bid.	No Change. Already eloborated in detail.
9	(ii) Cloud Management Software	2. Compute Virtualization 7.0	7. The solution should enforce security for virtual machines at the Ethernet layer. Disallow promiscuous mode, sniffing of network traffic, MAC address changes, and forged source MAC transmits.	7. Seems to be possible only with in kernel solutions which is specific to certain OEM, request you to reconsider this point.	No Change
10	(ii) Cloud Management Software	3. HCI (Storage Virtualization) 1.0	1. The solution should include storage virtualization / HCI software supporting all flash nodes which is Hardware independent to provide flexibility of choosing hardware from any x86 server manufacturer & should support mixing of different compatible x86 Server brands in same Cluster. Compatibility certification should be publicly endorsed by both, i.e. hardware OEM & Hyper Converged Software OEM.	1. Technically different brands can be part of single cluster, however, it is highly recommended in HCI environment to have different generation hardware from same OEM, request you to remove "& should support mixing of different compatible x86 Server brands in same Cluster. Compatibility certification should be publicly endorsed by both, i.e. hardware OEM & Hyper Converged Software OEM. (Need to check for VMware as well) " this part for better Life Cycle Management of hardware platform used for the cluster.	No Change

11	(ii) Cloud Management Software	3. HCI (Storage Virtualization) 2.0	2. Storage virtualization should support VM-Centric controls for managing storage service levels for capacity, IOPS, availability QoS by storage policy-based management and should not be dependent on LUNs. Should also support features like rack awareness, deduplication, compression & RAID 1 and RAID 5, 6 through erasure coding (for all flash). Support scale up by adding disk in the node without any additional licenses, scale out by adding nodes or entire racks. This addition of capacity should NOT result in an increase of the number of management points	Request you to change it as - 2. Should also support features like rack awareness, deduplication, compression & raid 5,6/equivalent through erasure coding (for all flash).	May be read as: 2. Storage virtualization should support VM-Centric controls for managing storage service levels for capacity, IOPS, availability QoS by storage policy-based management and should not be dependent on LUNs. Should also support features like rack awareness, deduplication, compression & RAID 1, 5, 6 or equivalent through erasure coding (for all flash). Support scale up by adding disk in the node without any additional licenses, scale out by adding nodes or entire racks. This addition of capacity should NOT result in an increase of the number of management points
12	(ii) Cloud Management Software	3. HCI (Storage Virtualization) 4.0	4. The solution shall provide a data caching tier that supports SSD, Ultra DIMM or NVMe and support for storage space efficiency features like de-duplication, compression and RAID 1 and RAID 5, 6 with erasure coding without dependence on any proprietary hardware.	Request you to change it as - 4. RAID 5/6 or equivalent with erasure coding without dependence on any proprietary hardware.	May be read as: 4. The solution shall provide a data caching tier that supports SSD, Ultra DIMM or NVMe and support for storage space efficiency features like de-duplication, compression and RAID 1, 5, 6 or equivalent with erasure coding without dependence on any proprietary hardware.
13	(ii) Cloud Management Software	3. HCI (Storage Virtualization) 8.0	8. The proposed software defined solution should use common storage management framework for HCI and traditional FC SAN, iSCSI & NAS Storage environment. Connect external 3rd party SAN/ NAS storage into the HCI cluster for capacity expansion and ease of migration from existing environment to HCI.	Request you to change it as - 8.The proposed software defined solution should use common storage management framework for HCI and traditional FC SAN/iSCSI & NAS Storage environment. Connect external 3rd party SAN/ NAS storage into the HCI cluster as additional data storage and ease of migration from existing environment to HCI.	No Change
14	(ii) Cloud Management Software	3. HCI (Storage Virtualization) 11.0	11. The solution shall provide ready to use templates to validate configuration standards on the platform covering security best practices, vendor hardening guidelines and regulatory mandates such as PCI-DSS, GDPR, FISMA and SOX to track & enforce compliance.	Request you to change it as - 11.The solution shall provide ready to use templates to validate configuration standards on the platform covering security best practices, vendor hardening guidelines and regulatory mandates such as PCI-DSS and SOX to track & enforce compliance. As GDPR & FISMA is applicable for Europe & USA respectively, request you to modify above clause.	May be read as: 11. The solution shall provide ready to use templates to validate configuration standards on the platform covering security best practices, vendor hardening guidelines and regulatory mandates such as PCI-DSS and SOX to track & enforce compliance.

15	(ii) Cloud Management Software	4. SDN (Network Virtualization) 2.0	2. The solution should provide distributed in-kernel/ integrated routing (BGP), VXLAN / GENEVE based logical virtual switching, NAT function, server load balancer, Software L2 bridging to physical environments, L2 & L3 VPN services, L2-L4 distributed stateful firewall at vNIC level and at a very granular level based on constructs such as MAC, IP, Ports, objects and tags, active directory groups, Security Groups and Security policies which must follow the VM in the event of migration (i.e. live migration).	Request you to change it as - 2.The solution should provide distributed in-kernel/ integrated routing (OSPF & BGP), VXLAN based logical virtual switching, NAT function, server load balancer, Software L2 bridging to physical environments, L2 & L3 VPN services, L2-L4 distributed stateful firewall at vNIC level and at a very granular level based on constructs such as MAC, IP, Ports, objects and tags, active directory groups, Security Groups and Security policies which must follow the VM in the event of migration (i.e. live migration). If proposed solution do not have requested features, can integrate 3rd party virtual appliances in order to achieve functionalities.	No Change. However agreed for "If proposed solution do not have requested features, can integrate 3rd party virtual appliances in order to achieve functionalities."
16	(ii) Cloud Management Software	4. SDN (Network Virtualization) 4.0	4. The solution should provide agentless guest introspection services like Anti-Malware etc and Network introspection services like IPS/ IDS, edge load balancing, multi-site networking (Layer 2 extension) irrespective of underlying physical topology for active DC & DR purposes, container network and security for container to container L3 networking & micro segmentation for micro services etc.	Request you to change it as - 4.The solution should provide agentless guest introspection services like Anti-Malware etc and Network introspection services like IPS/ IDS, edge load balancing, multi-site networking (Layer 2 extension) irrespective of underlying physical topology for active DC & DR purposes, container network and security for container to container L3 networking & micro segmentation for micro services etc.). If proposed solution do not have requested features, can integrate 3rd party virtual appliances in order to achieve functionalities.	No Change. However agreed for "If proposed solution do not have requested features, can integrate 3rd party virtual appliances in order to achieve functionalities."
17	(ii) Cloud Management Software	4. SDN (Network Virtualization) 6.0	6. The solution should protect every Virtual Machine with a stateful distributed firewall with Distributed IDPS and enable creation of security groups and security policies/ rules based on constructs like machine name, OS type, IP address, Logical Switches, Security Tags etc. and offer virtualized workload at the vNIC level to be protected with a full stateful firewall/IDPS engine at a very granular level based on constructs such as MAC, IP, Ports, objects and tags, active directory groups, Security Groups , etc.	Request you to change it as - 6.The solution should protect every Virtual Machine with a stateful distributed firewall with Distributed IDPS and enable creation of security groups and security policies/ rules based on constructs like machine name, OS type, IP address, Logical Switches, Security Tags etc. and offer virtualized workload at the vNIC level to be protected with a full stateful firewall/IDPS engine at a very granular level based on constructs such as MAC, IP, Ports, objects and tags, active directory groups, Security Groups , etc If proposed solution do not have requested features, can integrate 3rd party virtual appliances in order to achieve functionalities.	No Change. However agreed for "If proposed solution do not have requested features, can integrate 3rd party virtual appliances in order to achieve functionalities."
18	(ii) Cloud Management Software	4. SDN (Network Virtualization) 7.0	7. The solution should support for heterogeneous underlying infrastructure based on bare metal, KVM and VMware vSphere and provisioning of complete virtual/ SDN services irrespective of make and topology underlying physical network switches and routers.	7.The solution should support for heterogeneous underlying infrastructure based on bare metal, KVM and VMware vSphere and provisioning of complete virtual/ SDN services irrespective of make and topology underlying physical network switches and routers. Seems to be specific to certain OEM, request you to reconsider this point.	May be read as: 7. The solution should support for heterogeneous underlying infrastructure based on bare metal, multi-hypervisors, proposed hypervisor solution and provisioning of complete virtual/ SDN services irrespective of make and topology underlying physical network switches and routers.

19	(ii) Cloud Management Software	4. SDN (Network Virtualizatio n) 10.0	10. The solution should provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking services at Layer 2 through 7 such as DNAT/SNAT, DHCP and stateful firewall (L4 to L7) in addition to switching and routing (North-South and East-West).	Request youto change it as - 10.The solution should provide an integrated networking solution to provide advance turnkey container networking services at Layer 2 and stateful firewall in addition to switching.	No change
20	(ii) Cloud Management Software	4. SDN (Network Virtualizatio n) 12.0 - 15	12. The solution should be capable to provide multi-site networking (Layer 2 extension) irrespective of underlying physical topology for active DC & DR purposes, container network and security for container to container L3 networking and micro segmentation for microservices etc.	Request you to eloaborate these points in pre-bid.	No Change. Already eloborated in detail.
21	(ii) Cloud Management Software	4. SDN (Network Virtualizatio n) 17.0 - 18	17. Solution provide traffic visibility, end point monitoring for visibility up to layer 7 for network monitoring and automating application security rules, firewall planning & management, network virtualization operations & troubleshooting tools. 18. The solution should provide the application discovery (names, tags, RegEx), topology view, health checklist, edge load balance dashboard, DNS mapping (import bind file), and visibility across third-party switches, routers, firewalls and load balancers	Request you to eloaborate these points in pre-bid.	No Change. Already eloborated in detail.
22	(ii) Cloud Management Software	5. Cloud Platform 4.0	4. Solution should provide automation and orchestration solution for automated delivery of IaaS, PaaS, XaaS / SaaS services so that when VM/app is created it should automatically get the required virtualized compute, storage, switching, routing, firewall, load balancing services without any manual intervention. All compute, network, storage, security, load balancing policies must follow the life cycle of VM and movement within and across DC & DR.	Request you to eloaborate these points in pre-bid.	No Change. Already eloborated in detail.
23	(ii) Cloud Management Software	5. Cloud Platform 9.0	9. The solution should have Life Cycle Management Work flows: Provisioning, Day-2 operations like cloning, re-sizing, snapshot, deletion etc. There should be zero manual intervention in this entire process across Private and Public Cloud (AWS, Azure, GCP). The software must allow the designer canvas to drag and drop Private and Public Cloud (AWS, Azure, & GCP) including Kubernetes resources to design the blueprints	Request you to remove - Day-2 operations like cloning, re-sizing, snapshot, deletion etc.	No Change.
24	(ii) Cloud Management Software	5. Cloud Platform 13.0	13. The solution should provide for creation of complete application blueprints along with required virtual networking (routing, load balancing) and security services for the application using a user-friendly graphical interface by using drag & drop functionality. Allow mixed deployment in a blueprint. E.g., Provision database, Provision Application & Web Servers from a single blueprint.	Request you to modify it as - 13.The solution should provide for creation of complete application blueprints along with required basic virtual networking	No Change. If proposed solution do not have requested features, can integrate 3rd party virtual appliances in order to achieve functionalities.

25	(ii) Cloud Management Software	5. Cloud Platform 14.0	14. The solution should reduce cost and improve efficiency with real-time, ML-based capacity and cost analytics. Deliver optimal consolidation and proactive planning using a real-time, forward-looking capacity analytics engine, predict future demand and provide actionable recommendations that include reclamation, procurement and cloud migration planning options.	Request you to modify it as - 14.The solution should reduce cost and improve efficiency with real-time, ML-based capacity and cost analytics. Deliver optimal consolidation and proactive planning using a real-time, forward-looking capacity analytics engine, predict future demand and provide actionable recommendations that include reclamation, procurement.	May be read as: 14. The solution should reduce cost and improve efficiency with real-time, ML-based capacity and cost analytics. Deliver optimal consolidation and proactive planning using a real-time, forward-looking capacity analytics engine, predict future demand and provide actionable recommendations that include reclamation, procurement.
26	(ii) Cloud Management Software	5. Cloud Platform 16.0	16. The solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc.	Request you to modify it as - 16.The solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc.	No Change.
27	(ii) Cloud Management Software	5. Cloud Platform 19.0	19. The solution should provide cloud agnostic templates to deploy resources on private and public clouds (AWS, Azure, Google Cloud) with Infrastructure as Code and native cloud resources via a plugin-based framework.	Request you to modify it as - 19.The solution should provide cloud agnostic templates to deploy resources on private and public clouds (AWS, Azure, Google Cloud) with Infrastructure as Code and native cloud resources.	May be read as: 19. The solution should provide cloud agnostic templates to deploy resources on private and public clouds (AWS, Azure, Google Cloud) with Infrastructure as Code and native cloud resources.
28	(ii) Cloud Management Software	5. Cloud Platform 21.0	21. The solution should provide flexibility in deployment with having cloud-independent VM/application profile coupled with its cloud-specific logic that abstracts the application from the specific cloud, interprets the needs of the application, and translates those logical needs to cloud-specific services and APIs. The tool should eliminate the need of cloud specific scripting/IaaS to prevent cloud lock-in.	Request you to modofy it as - 21.The solution should provide flexibility in deployment with having cloud-independent VM/application.	May be read us: 21. The solution should provide flexibility in deployment with having cloud-independent VM/application.
29	(ii) Cloud Management Software	5. Cloud Platform 22.0	22. The solution should provide native integration with cloud automation layer on premise and public cloud and fully supported Ansible modules, fully supported Terraform provider and PowerShell integration. RESTful API based on JSON for integration with cloud management platforms, DevOps automation tools and custom automation.	Request you to modofy it as - 22.The solution should provide native integration with cloud automation layer on premise and public cloud and fully supported Ansible modules, fully supported Terraform provider. RESTful API based on JSON for integration with cloud management platforms, DevOps automation tools and custom automation.	No Change.
30	(ii) Cloud Management Software	5. Cloud Platform 23.0	23. The solution should automate the application and infrastructure delivery process with release pipeline management, including visibility and analytics into active pipelines and their status for troubleshooting and leverage existing tools and processes with out-of-the-box integration such as Ansible, Bitbucket, Github, Gitlab, IPAM, Puppet, Openshift, salt, terrafomr, bamboo, Docker, Docker Registry, GIT, Jenkins, Jira and TFs etc	Request you to modofy it as - 23.The solution should automate the application and infrastructure delivery process with release pipeline management, including visibility and analytics into active pipelines and their status for troubleshooting and leverage existing tools and processes with out-of-the-box integration such as Ansible, Openshift, terrafomr, Jenkins, etc	No Change.

31	(ii) Cloud Management Software	5. Cloud Platform 25.0	25. Should support in built CI/CD tool for devsecops to automate build, release and deploy from continuous and repeatable basis by integrating on prem cloud across VMs and containers. Should be able to track artifacts and automate deployment configurations to ensure correct versions are used across all stages of the development lifecycle.	Request you to eloaborate these points in pre-bid meeting	No Change. Already eloborated in detail.
32	(ii) Cloud Management Software	5. Cloud Platform 26.0	26. The solution should provide out-of-the-box monitoring and troubleshooting for Packaged applications with Open Source Telegraf Agent and application performance management tool integrations.	Request you to remove this point	No Change.
33	(ii) Cloud Management Software	5. Cloud Platform 27.0 - 32	27. The solution should allow connecting to data-center ecosystem components e.g., operating systems, applications, servers, storage arrays, firewalls, network devices, etc., providing a single location to collect, store, and analyze logs at scale. 28. The solution should provide intelligent log analytics to be able to bring unstructured and structured data together, for enhanced end-to-end operations management, collect and analyze all types of machine-generated log data, for example, network traces, configuration files, messages, performance data, system state dumps, and more. 29. The solution should provide real-time predictive capacity management, including trending, metering, rightsizing, optimization, super metrics, metric correlation, relationship mapping, business and operational intent-based automated and schedulable workload balancing and optimization. 30. The solution should have log analytics available in one single management window to make troubleshooting easier. Should provide a single location to collect, store, and analyze unstructured data from OS, VMs, apps, storage, network devices, containers, Kubernetes etc. at scale. Should provide intuitive dashboard and should allow IT teams to search for certain event patterns & types for troubleshooting. 31. The solution should be able to add all types of structured and unstructured log data, enabling administrators to troubleshoot quickly, without needing to know the data beforehand, perform long term Log retention and Log archival for future access and centralize log storage and analytics feature with Dashboards, Reports and Alerts with Webhook integration for Automated Remediation 32. The solution should utilize predictive analytics, machine learning and root cause analysis tools across physical, virtual and multi-cloud environments for faster problem resolution and automatically choose the best visualization for data, saving time, pinpoints and tracks potential issues	Request you to eloaborate these points in pre-bid meeting	No Change. Already eloborated in detail.
34	(ii) Cloud Management Software	5. Cloud Platform 34	34. The solution shall preemptively rebalance workloads in advance of upcoming demands and spikes, eliminating resource contention before it happens thus ensuring that workloads get the resources that they need at all times and also provide smart Alerts, guided remediation, self-learning analytics with dynamic thresholds to deliver recommendations, or trigger actions, that optimize performance and capacity and enforce configuration standards.	Request you to eloaborate these points in pre-bid meeting	No Change. Already eloborated in detail.

35	(ii) Cloud Management Software	6. DR Solution 12.0	12. "From initial setup to ongoing management, DR solution should deliver simple and policy-based operations: a. Centralized recovery plans to create and manage recovery plans for thousands of VMs directly from the intuitive HTML5 user interface. b. Policy-based management to utilize storage profile protection groups to identify protected storage, automate the process of protecting and unprotecting VMs, and adding and removing storage from protection groups. c. Self-service provisioning to allow application tenants to provision DR protection using blueprints in Automation layer."	Request you to remove below point •Self-service provisioning to allow application tenants to provision DR protection using blueprints in Automation layer	No Change.
36	(ii) Cloud Management Software	6. DR Solution 13.0 / h	13. "The solution should offer: Support for array-based replication offers choice and options for replication with zero data loss."	Request you to modofy it as - h. Support for array-based replication /software defined replication offers choice and options for replication with zero data loss." Change required	No Change.
37	(ii) Cloud Management Software	6. DR Solution 14.0 - 17 & 19	14. "The solution should Map virtual machines to appropriate resources on the failover site a. Option to customize the shutdown of low-priority virtual machines at the failover site to get more resources or proper utilization of resources"" b. Option to recover multiple sites into a single shared recovery site c. Automatically stop replication between sites and promotion of replicated storage for recovery. d. The solution should provide technology so that live migration of virtual machine disks would be supported between different storages and provide distributed resource scheduling of storage" 15. The solution should be storage-agnostic replication that supports use of low-end storage, including direct-attached storage and also provides host based replication which will replicate only changed blocks to increase network efficiency. 16. The solution should provide flexibility and choice through native integration with hypervisor/ VM based Replication, Virtual Volumes (vVols), and array-based replication solutions from all major storage partners. 17. The solution should provide automatic generation of history reports after the completion of workflows such as a recovery plan test and clean-up are performed in DR solution. These reports should document items such as the workflow name, execution times, successful operations, failures, and error messages which are useful for internal auditing, proof of disaster recovery protection for regulatory requirements, and troubleshooting. Reports can be exported to HTML, XML, CSV, Microsoft Excel, Word document. 19. The solution should be able to provide minimum of 5 mins RTO & RPO.	Request you to eloaborate these points in pre-bid meeting	No Change. Already eloborated in detail.

38	(ii) Cloud Management Software	BoQ - Licenses	Quantity Delivery at Hyderabad: For 8 Nodes at SN. 1 (4+4) DC DR config Quantity Delivery at Noida: For 4 Nodes at SN. 1	The number of Servers asked under "SN.1 Servers / HCI " are 13 server at Hyderabad and 7 at Noida. Whereas, the Cloud Management software licenses in SN.2 is asked only for 8 Nodes at Hyderabad and 4 Nodes at Noida. Please clarify how the remaining servers will be consumed. Please clarify if server resources required for cloud management components have been factored in these new servers asked in RFP and resources from these servers can be utilized to deploy management components.	The remaining servers are to be utilized for some other purpose. Cloud Management components has to be implemented in the same compute clusters.
39	(ii) Cloud Management Software	7. Installation & Testing	1. Direct installation by OEM Professional as per the Scope of Work mentioned in the document 2. OEM has to provide the test cases as per the defined scope of work and demonstrate the required features during testing for successful	We request to you kindly allow bidder to do the installation as SI also have the skills to deliver the solutions. Please allow installation by certified engineer of OEM or bidder	No Change
40	(ii) Cloud Management Software	8. Training & Certification	OEM has to provide on-site training on the Cloud & DC-DR replication, Network & Security minimum of 2 weeks for around 20 members along with certification exam coupons.	Please allow that on-site training is provided by a certified engineer, either from the OEM or the bidder, and that it includes a certification exam.	No Change
41	(v) NVMe Storage	1. Connectivity / Port	2. Minimum of 8 Nos. of FC Ports of 32 Gbps or higher speed and 4 Nos. of 10/25 Gbps iSCSI ports expandable to 16 Nos. of FC and 8 Nos. of iSCSI	Post scalabilitiy can be achieved by scaling out the storage. Kindly change this clause to " 2. Minimum of 8 Nos. of FC Ports of 32 Gbps or higher speed and 4 Nos. of 10/25 Gbps iSCSI ports." Minimum of 8 Nos. of FC Ports of 32 Gbps or higher speed and 4 Nos. of 10/25 Gbps iSCSI ports	May be read as: 2. Minimum of 8 Nos. (expandable to 16 Nos.) of FC Ports of 32 Gbps or higher speed and 4 Nos. of 10/25 Gbps iSCSI ports and NAS
42	(v) NVMe Storage	1. Connectivity / Port	3. Back end ports min 4 Nos. of 12 Gbps SAS or higher	Back end ports min 4 Nos. 100GbE ports 3..Back end ports min 4 Nos. of 16 Gbps NVMe or higher	May be read as: 3. Back end ports min 4 Nos. of 100 Gbps or higher Ethernet / PCI / Infiband NVMe
43	(v) NVMe Storage	1. Connectivity / Port	4. Min 2 FC / Ethernet of 10 Gbps or higher for dedicated remote replication ports	We don't need different ports for replication. Same frontend port can be used for replication as well. Please delete.	No Change Please delete
44	(v) NVMe Storage	1. Connectivity / Port	New point added	New point added	New point added 5. Storage should support NAS and required license to be provided for full capacity from Day one.
45	(v) NVMe Storage	3. Data Replication	1. Should support both Synchronous and Asynchronous replication methods. Asynchronous replication has to be configured from day one. All replication licenses should be included for full capacity from day one.	Should support Asynchronous replication methods. Asynchronous replication has to be configured from day one. All replication licenses should be included for full capacity from day one	May be read as: 1. Should support both Synchronous / Asynchronous replication methods. Asynchronous replication has to be configured from day one. All replication licenses should be included for full capacity from day one.

46	(v) NVMe Storage	4. Capacity, Disks & RAID configuratio n	1. Usable capacity of the Storage is 100 TB in RAID 5 (with not more than 8 disks in a group) without considering any DRR features like Dedup or Compression. The individual NVMe disk drive capacity should not be more than 16TB.	Please allow vendors to quote bigger capacity NVMe drives as well. This will help to meet the scale with the intermix of NVMe and SAS SSDs. Kindly change this clause to " 1. Usable capacity of the Storage is 100 TB in RAID 5 (with not more than 8 disks in a group) without considering any DRR features like Dedup or Compression ."	May be read as: 1. Usable capacity of the Storage is 100 TB in RAID 6 (with not more than 10 disks in a group) without considering any DRR features like Dedup or Compression. The individual NVMe disk drive capacity should not be more than 16TB.
47	(v) NVMe Storage	4. Capacity, Disks & RAID configuratio n	2. Storage should be expandable up to 1 PB. The usable capacity NVMe (with drives less than 16 TB) should be expandable to capacity up to 250TB	Request to remove the restriction on drive size. Help to reduce the total footprint of DC with perfroamce assurance. Kindly change this clause to " 2. Storage should be expandable up to 1 PB. The usable capacity NVMe should be expandable to capacity up to 250TB." Kindly amend the clause as below- Storage should be expandable up to 1 PB. The usable capacity NVMe (with less than 16 TB NVMe TLC/MLC drive) should be expandable to capacity up to 250 TB.	May be read as: 2. Storage should be expandable up to 1 PB usable capacity (with NVMe drives less than 16 TB).
48	(v) NVMe Storage	4. Capacity, Disks & RAID configuratio n	4. Should support both SSD (SAS connector) and NVMe Disks	Should support NVMe Disks Kindly amend the clause as below - Should support NVMe Disks and NVMe backend.	May be read as: 4. Should support NVMe Disks
49	(v) NVMe Storage	4. Capacity, Disks & RAID configuratio n	6. Automated Storage Tiering feature across the NVMe and SSD Drives types and all the required license has to be included.	Request to remove this clause. Kindly amend the clause as below - Storage should support adaptive data reduction technology (ADR) 2:1	Clause removed
50	(v) NVMe Storage	4. Capacity, Disks & RAID configuratio n	7. The supplied disk (wear & tear) and data should be comprehensively covered under the warranty of Storage	Warranty can cover the Disk drives however data is being protected using RAID technology and other protection mechanism.. Kindly change this clause to " 7. The supplied disk (wear & tear) should be comprehensively covered under the warranty of Storage. "	No Change.
51	(v) NVMe Storage	7. Performance & Availability	4. The storage should deliver 200 K IOPS with latency less than 0.7 ms maximum from day one at a bandwidth of 4 GBps.	4. The storage should deliver 200 K 150K IOPS with latency less than 0.7 ms 3ms maximum from day one at a bandwidth of 4 GBps.For the mentioned capacity, best possible IOPS and latency is mentioned. This can be increased further with scale-up/scale-out. Kindly amend the clause as below- The storage should deliver 200 K IOPS @70:30 r/w on 8K block size with latency less than 0.7 ms maximum from day one at a bandwidth of 4 GBps.	4. The storage should deliver 200 K IOPS @ 70:30 R:W with latency less than 0.7 ms maximum from day one at a bandwidth of 4 GBps.

52	(vi) SAN Switch	4. Warranty & Support	Warranty & Support / The quoted model of SAN Switch should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF	Kindly modify it to "The quoted model of SAN Switch should have support life of 7 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF. Reason as per the industry , OEM support maximum 7 year, we request to modify the clasue.	May be read as: Warranty & Support / The quoted model of SAN Switch should have support life of 7 years minimum from the the date of handover (after successful commissioning of solution) to C-DAC, same need to be confirmed in signed MAF
53	(vii) SDN Solution – Network Leaf Switch - 48px10G-BASE-T, 4px40/100G	3. Performance requirement	9. Switch should support minimum 3 Tbps of switching throughput	As the ports asked are 48x10G and 4x100G, which requires 1760 Gbps throughput at line rate. So kindly, change the clause as "9. Switch should support minimum 1.76 Tbps of switching throughput" With the port requirement that has been asked in the RFP, 3Tbps of throughput is not required from a copper based 10G switch. Kindly modify it to " Switch should support minimum 2 Tbps of switching throughput	May be read as: 9. Switch should support minimum 1.76 Tbps of switching throughput
54	(vii) SDN Solution – Network Leaf Switch - 48px10G-BASE-T, 4px40/100G	9. Manageabilit y	9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop with reason of drop c. Per Flow latency (per switch and end to end)	The "reason for drop" in b. is OEM specific, so please change the clause as below for wider OEM particiaption "9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop c. Per Flow latency (per switch and end to end)"	May be read as: 9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop c. Per Flow latency (per switch and end to end)
55	(vii) SDN Solution – Network Leaf Switch - 48px10G-BASE-T, 4px40/100G	11. General Requirement s	6. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring	Kindly modify it to " All Data Center Network switches should be able to be managed from Single Dashboard for ease of Management and Monitoring"	May be read as: 6. All Data Center Network switches should be able to be managed from Single Dashboard for ease of Management and Monitoring
56	(vii) SDN Solution – Network Leaf Switch - 48px10G-BASE-T, 4px40/100G	14. Warranty	2. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF	Kindly modify it to " All Network Switches & Routers quoted Models should have support life of 7 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF". Reason as per the industry , OEM support maximum 7 year, we request to modify the clasue.	May be read as: Warranty & Support - All Network Switches & Routers quoted Models should have support life of 7 years minimum from the the date of handover (after successful commissioning of solution) to C-DAC, same need to be confirmed in signed MAF
57	(viii) SDN Solution – Network Leaf Switch - 48px10G (Fibre / Copper), 4px40/100G	3. Performance requirement	9. Switch should support minimum 3 Tbps of switching throughput	As the ports asked are 48x25G and 4x100G, which requires 3200 Gbps throughput at line rate. So kindly, change the clause as "9. Switch should support minimum 3.2 Tbps of switching throughput"	No Change.

58	(viii) SDN Solution – Network Leaf Switch - 48px10G (Fibre / Copper), 4px40/100G	9. Manageabilit y	9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop with reason of drop c. Per Flow latency (per switch and end to end)	The "reason for drop" in b. is OEM specific, so please change the clause as below for wider OEM particiaption "9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop c. Per Flow latency (per switch and end to end)"	May be read as: 9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop c. Per Flow latency (per switch and end to end)
59	(viii) SDN Solution – Network Leaf Switch - 48px10G (Fibre / Copper), 4px40/100G	11. General Requirement s	6. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring	Kindly modify it to " All Data Center Network switches should be able to be managed from Single Dashboard for ease of Management and Monitoring"	May be read as: 6. All Data Center Network switches should be able to be managed from Single Dashboard for ease of Management and Monitoring
60	(viii) SDN Solution – Network Leaf Switch - 48px10G (Fibre / Copper), 4px40/100G	14. Warranty	2. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF	Kindly modify it to " All Network Switches & Routers quoted Models should have support life of 7 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF". Reason as per the industry , OEM support maximum 7 year, we request to modify the clasue.	May be read as: Warranty & Support - All Network Switches & Routers quoted Models should have support life of 7 years minimum from the the date of handover (after successful commissioning of solution) to C-DAC, same need to be confirmed in signed MAF
61	(ix) SDN Solution – Network Spine Switch - 48px40/100G	9. Manageabilit y	5. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop with reason of drop c. Per Flow latency (per switch and end to end)	The "reason for drop" in b. is OEM specific, so please change the clause as below for wider OEM particiaption "9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop c. Per Flow latency (per switch and end to end)"	May be read as: 5. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop c. Per Flow latency (per switch and end to end)
62	(ix) SDN Solution – Network Spine Switch - 48px40/100G	1. General Requirement s	7. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring	Kindly modify it to " All Data Center Network switches should be able to be managed from Single Dashboard for ease of Management and Monitoring"	May be read as: 7. All Data Center Network switches should be able to be managed from Single Dashboard for ease of Management and Monitoring
63	(ix) SDN Solution – Network Spine Switch - 48px40/100G	14. Warranty	2. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF	Kindly modify it to " All Network Switches & Routers quoted Models should have support life of 7 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF". Reason as per the industry , OEM support maximum 7 year, we request to modify the clasue.	May be read as: Warranty & Support - All Network Switches & Routers quoted Models should have support life of 7 years minimum from the the date of handover (after successful commissioning of solution) to C-DAC, same need to be confirmed in signed MAF

64	(x) SDN Solution – Network Access / Management Switch - 48px1G (BaseT), 4px10G (BaseT)	7. Manageability	9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop with reason of drop c. Per Flow latency (per switch and end to end)	The "reason for drop" in b. is OEM specific, so please change the clause as below for wider OEM particiaption "9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop c. Per Flow latency (per switch and end to end)"	May be read as: 9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop c. Per Flow latency (per switch and end to end)
65	(x) SDN Solution – Network Access / Management Switch - 48px1G (BaseT), 4px10G (BaseT)	8. General Requirements	6. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring	Kindly modify it to " All Data Center Network switches should be able to be managed from Single Dashboard for ease of Management and Monitoring"	May be read as: 6. All Data Center Network switches should be able to be managed from Single Dashboard for ease of Management and Monitoring
66	(x) SDN Solution – Network Access / Management Switch - 48px1G (BaseT), 4px10G (BaseT)	11. Warranty	2. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF	Kindly modify it to " All Network Switches & Routers quoted Models should have support life of 7 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF". Reason as per the industry , OEM support maximum 7 year, we request to modify the clasue.	May be read as: Warranty & Support - All Network Switches & Routers quoted Models should have support life of 7 years minimum from the the date of handover (after successful commissioning of solution) to C-DAC, same need to be confirmed in signed MAF
67	(xi) Router (2x10G, 4x1G)	1. Interface	1. Router should have the following interfaces: a. Min. 4p x 1 Gbps or higher which supports SFP / SFP-BASET transceivers on all ports, populated with 4 Nos. of SFP. Also supply 2 Nos. of SFP-BASET for interoperability of existing copper links. b. Min. 2p x 10 Gbps or higher ports which supports SFP / SFP-BASET / SFP+ / SFP+10GBASE-T transceivers on all ports, populated with 2 Nos. of SFP+ c. Router should have additional interface modules / slot support for future expansion of Min. 2p x 10 Gbps or higher ports or Min. 4p x 1 Gbps or higher d. All the ports mentioned in S.N. a, b & c should be WAN ports e. Router should have 1x RJ45 console port for management	Reques to modify the clause a " 1. Router should have the following interfaces: a. Min. 4p x 1 Gbps or higher which supports SFP / SFP-BASET transceivers on all ports, populated with 4 Nos. of SFP. Also supply 2 Nos. of SFP-BASET for interoperability of existing copper links. b. Min. 2p x 10 Gbps or higher ports which supports SFP / SFP-BASET / SFP+ transceivers on all ports, populated with 2 Nos. of SFP+ c. Router should have additional interface modules / slot support for future expansion of Min. 2p x 10 Gbps or higher ports or Min. 4p x 1 Gbps or higher d. All the ports mentioned in S.N. a, b & c should be WAN ports e. Router should have 1x RJ45 console port for management	Clause 1. b. May be read as: b. Min. 2p x 10 Gbps or higher ports which supports SFP / SFP-BASET / SFP+ transceivers on all ports, populated with 2 Nos. of SFP+
68	(xi) Router (2x10G, 4x1G)	2. Performance requirement	1. The Device must support minimum 128 concurrent IPsec tunnel with AES 256 encryption expandable to 256 tunnels in future.	The IPSEC tunnels must be terminated on firewall and router should be catering to the core functionality of routing. So request you to please remove this clause.	No Change. Solution can be offered with additional hardware also.
69	(xi) Router (2x10G, 4x1G)	2. Performance requirement	2.Device should include a minimum 2 Gbps IPsec throughput	The IPSEC tunnels must be terminated on firewall and router should be catering to the core functionality of routing. So request you to please remove this clause.	No Change. Solution can be offered with additional hardware also.
70	(xi) Router (2x10G, 4x1G)	2. Performance requirement	4.Device should support minimum 5 Gbps IPv4 encrypted throughput.	The encryption and decryption should be done on firewall and router should be catering to the core functionality of routing. So request you to please remove this clause.	No Change. Solution can be offered with additional hardware also.

71	(xi) Router (2x10G, 4x1G)	2. Performance requirement	5.Device should support minimum 4 million IPv4 & 4Million IPv6 routes.	As the number of IPv6 routes is on higher side, while the number of IPv6 routes even in internet are not that high. So, we request to please change the clause as below for wider OEM particiaption. "**Device should support minimum 4 million IPv4 routes and 1 Million IPv6 routes.**"	May be read as: 5. Device should support minimum 4 million IPv4 & 1 Million IPv6 routes
72	(xi) Router (2x10G, 4x1G)	2. Performance requirement	9.Hardware should be able to work as traditional router and capable of upgrading to SDWAN router.	As we have a separate box for SD-WAN and for high scale routing we have a separate router, so request to remove this clause for Arista to qualify and bid, or give Arista option to quote separate box for SDWAN functionality for future requirement and can integrated and managed from Same SDN dashboard.	No Change. Solution can be offered with additional hardware also.
73	(xi) Router (2x10G, 4x1G)	4. Security	1.AES-128, or AES-256 Encryption	The encryption and decryption should be done on firewall and router should be catering to the core functionality of routing. So request you to please remove this clause.	No Change. Solution can be offered with additional hardware also.
74	(xi) Router (2x10G, 4x1G)	5. Networking and Routing	2.Device Should support Static NAT, Dynamic NAT, NAPT	Functionality related with security like NAT should be offloaded to firewall instead of keeping on router.Router should be kept specifically for routing purpose. So, request to please remove this clause.	No Change. Solution can be offered with additional hardware also.
75	(xi) Router (2x10G, 4x1G)	5. Networking and Routing	6.Proposed router should support SD-WAN functionality as well without changing the hardware in the setup.	As we have a separate box for SD-WAN and for high scale routing we have a separate router, so request to remove this clause for Arista to qualify and bid, or give Arista option to quote separate box for SDWAN functionality for future requirement and can integrated and managed from Same SDN dashboard.	No Change. Solution can be offered with additional hardware also.
76	(xi) Router (2x10G, 4x1G)	6. Manageabilit y	4. Device should support management and monitoring status using different type of Industry standard NMS using SNMP v1 and v2, SNMP v3 with Encryption.	Need clarification as Encryption would be supprted only with SNMPv3. Request for your clarification.	No Change. Encryption for SNMPv3 only.
77	(xi) Router (2x10G, 4x1G)	7. General requirements	5. Visibility & Automation: All Network switches & routers should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution. The solution should be compatible and integrated with the proposed cloud solution.	Request to remove the clause.	Clause removed
78	(xi) Router (2x10G, 4x1G)	7. General requirements	6. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring	Request to remove the clause.	Clause removed
79	(xi) Router (2x10G, 4x1G)	9. Scope of supply installation & management	4. Router should be configured in HA mode with Active-Active configurations.	Request to modify the clause as "4. Router should be configured in HA mode with Active-Active /Active-Standy configurations.	May be read as: 4. Router should be configured in HA mode with Active-Active /Active-Standy configurations.

80	(xii) Router(4x10G,4x1G)	1. Interface	1. Router should have the following interfaces: a. Min. 4p x 1 Gbps or higher which supports SFP / SFP-BASET transceivers on all ports, populated with 4 Nos. of SFP. Also supply 2 Nos. of SFP-BASET for interoperability of existing copper links. b. Min. 4p x 10 Gbps or higher ports which supports SFP / SFP-BASET / SFP+ / SFP+10GBASE-T transceivers on all ports, populated with 2 Nos. of SFP+ c. Router should have additional interface modules / slot support for future expansion of Min. 4p x 10 Gbps or higher ports or Min. 4p x 1 Gbps or higher d. All the ports mentioned in S.N. a, b & c should be WAN ports e. Router should have 1x RJ45 console port for management	Reques to modify the clause a " "4. Router should have the following interfaces: a. Min. 4p x 1 Gbps or higher which supports SFP / SFP-BASET transceivers on all ports, populated with 4 Nos. of SFP. Also supply 2 Nos. of SFP-BASET for interoperability of existing copper links. b. Min. 4p x 10 Gbps or higher ports which supports SFP / SFP-BASET / SFP+ transceivers on all ports, populated with 2 Nos. of SFP+ c. Router should have additional interface modules / slot support for future expansion of Min. 4p x 10 Gbps or higher ports or Min. 4p x 1 Gbps or higher d. All the ports mentioned in S.N. a, b & c should be WAN ports e. Router should have 1x RJ45 console port for management"	Clause 1. b. May be read as: b. Min. 2p x 10 Gbps or higher ports which supports SFP / SFP-BASET / SFP+ transceivers on all ports, populated with 2 Nos. of SFP+
81	(xii) Router(4x10G,4x1G)	2. Performance requirement	5. The Device must support minimum 128 concurrent IPsec tunnel with AES 256 encryption expandable to 256 tunnels in future.	The IPSEC tunnels must be terminated on firewall and router should be catering to the core functionality of routing. So request you to please remove this clause.	No Change. Solution can be offered with additional hardware also.
82	(xii) Router(4x10G,4x1G)	2. Performance requirement	6.Device should include a minimum 2 Gbps IPsec throughput	The IPSEC tunnels must be terminated on firewall and router should be catering to the core functionality of routing. So request you to please remove this clause.	No Change. Solution can be offered with additional hardware also.
83	(xii) Router(4x10G,4x1G)	2. Performance requirement	8.Device should support minimum 5 Gbps IPv4 encrypted throughput.	The encryption and decryption should be done on firewall and router should be catering to the core functionality of routing. So request you to please remove this clause.	No Change. Solution can be offered with additional hardware also.
84	(xii) Router(4x10G,4x1G)	2. Performance requirement	9.Device should support minimum 4 million IPv4 & 4Million IPv6 routes.	As the number of IPv6 routes is on higher side, while the number of IPv6 routes even in internet are not that high. So, we request to please change the clause as below for wider OEM particiaption. "**Device should support minimum 4 million IPv4 routes and 1 Million IPv6 routes.**"	May be read as: 5. Device should support minimum 4 million IPv4 & 1 Million IPv6 routes
85	(xii) Router(4x10G,4x1G)	2. Performance requirement	13.Hardware should be able to work as traditional router and capable of upgrading to SDWAN router.	As we have a separate box for SD-WAN and for high scale routing we have a separate router, so request to remove this clause for Arista to qualify and bid, or give Arista option to quote separate box for SDWAN functionality for future requirement and can integrated and managed from Same SDN dashboard.	No Change. Solution can be offered with additional hardware also.
86	(xii) Router(4x10G,4x1G)	4. Security	8.AES-128, or AES-256 Encryption	The encryption and decryption should be done on firewall and router should be catering to the core functionality of routing. So request you to please remove this clause.	No Change. Solution can be offered with additional hardware also.
87	(xii) Router(4x10G,4x1G)	5. Networking and Routing	2.Device Should support Static NAT, Dynamic NAT, NAPT	Functionality related with security like NAT should be offloaded to firewall instead of keeping on router.Router should be kept specifically for routing purpose. So, request to please remove this clause.	No Change. Solution can be offered with additional hardware also.
88	(xii) Router(4x10G,4x1G)	5. Networking and Routing	8.Proposed router should support SD-WAN functionality as well without changing the hardware in the setup.	As we have a separate box for SD-WAN and for high scale routing we have a separate router, so request to remove this clause for Arista to qualify and bid, or give Arista option to quote separate box for SDWAN functionality for future requirement and can integrated and managed from Same SDN dashboard.	No Change. Solution can be offered with additional hardware also.

89	(xii) Router(4x10G,4x1G)	6. Manageability	4. Device should support management and monitoring status using different type of Industry standard NMS using SNMP v1 and v2, SNMP v3 with Encryption.	Need clarification as Encryption would be supprted only with SNMPv3. Request for your clarification.	No Change. Encryption for SNMPv3 only.
90	(xii) Router(4x10G,4x1G)	7. General requirements	5. Visibility & Automation: All Network switches & routers should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution. The solution should be compatible and integrated with the proposed cloud solution.	Request to remove the clause.	Clause removed
91	(xii) Router(4x10G,4x1G)	7. General requirements	6. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring	Request to remove the clause.	Clause removed
92	(xii) Router(4x10G,4x1G)	9. Scope of supply installation & management	4. Router should be configured in HA mode with Active-Active configurations.	Request to modify the clause as "4. Router should be configured in HA mode with Active-Active /Active-Standy configurations.	May be read as: 4. Router should be configured in HA mode with Active-Active /Active-Standy configurations.
93	General/New	General/New	SDN Controller Specs is Missing in the Specification	SDN Controller Specs is Missing in the Specification	Fabric SDN Controller specs with multi-hypervisor solution attached.
94	(xiii) EDR Solution (Servers) & (xiv) EDR Solution (Desktops)	3. Agent Features	7. The proposed solution should automatically remove old agents from console, if agent haven't communicated to the management console for a configurable period of time.	The proposed solution should automatically remove old agents from console	No Change.
95	(xiii) EDR Solution (Servers) & (xiv) EDR Solution (Desktops)	5. Response & Remediation Capabilities	1. The proposed solution should support full remote shell for all OS (Windows, Linux & Mac) and not limited or restricted to set of commands.	The proposed solution should support sweep method across for all OS (Windows, Linux & Mac) to scan for IOC's across the deployment.	Clause removed
96	(xiii) EDR Solution (Servers) & (xiv) EDR Solution (Desktops)	5. Response & Remediation Capabilities	2. The proposed solution should track all remote shell commands and logged during a remote shell session.	The proposed solution should track all commands/activities/process details and logged on the end user system.	Clause removed
97	(xiii) EDR Solution (Servers) & (xiv) EDR Solution (Desktops)	5. Response & Remediation Capabilities	6. The proposed solution should have the ability to remediate all operating system changes and perform corrective action in machine speed. The solution should also be able to undo any system level changes related to the attack such as Registry edits, configuration changes etc.	To be Deleted	Clause removed
98	(xiii) EDR Solution (Servers) & (xiv) EDR Solution (Desktops)	5. Response & Remediation Capabilities	7. The proposed solution should reverse destructive data event but not limited to ransomware. The solution should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state.	To be Deleted	Clause removed

99	(xiii) EDR Solution (Servers) & (xiv) EDR Solution (Desktops)	6. Policy & Installation	16.The proposed solution shall support static (Hash, IP, Domain) and dynamic behavior (Attack Pattern) IOCs	Kindly change this clause to " The proposed solution shall support static (Hash) and dynamic behaviour (Attack Pattern) IOCs "	No Change.
100	(xiii) EDR Solution (Servers)	6. Policy & Installation	19.The proposed solution shall not limit to only endpoint but also able to show and correlate network data.	Kindly remove this clause, A its not applicable for on on-prem solution	No Change.
101	(xiii) EDR Solution (Servers) & (xiv) EDR Solution (Desktops)	10. Device & Network Discovery	1. The solution should automatically discover devices in a network without the need to deploy sensors.	The solution should automatically discover devices in a network by integrating with network access controller/gateway	May be read as: The solution should automatically discover devices in a network by integrating with network access controller/gateway
102	(xiii) EDR Solution (Servers) & (xiv) EDR Solution (Desktops)	10. Device & Network Discovery	3. The proposed solution must have rogue devices discovery capability to reduce the potential attack surface.	To be Deleted	Clause removed
103	(xiii) EDR Solution (Servers) & (xiv) EDR Solution (Desktops)	12. Integration	1. The solution must Integrate with Active Directory for automatic Agent to Group Mappings and policy association. The solution management server should not have any dependencies on the AD state. The product should support multiple Active Directory domains and forests.	The solution must Integrate with Active Directory for automatic or manual Agent to Group Mappings and policy association. The solution management server should not have any dependencies on the AD state if integrating with AD	May be read as: The solution must Integrate with Active Directory for automatic or manual Agent to Group Mappings and policy association. The solution management server should not have any dependencies on the AD state if integrating with AD
104	(xv) DDoS (Hardware Appliance)	1. Type	1. The proposed solution should have dedicated DDoS protection device (NOT be a part of Application Delivery Controller, Router, UTM, Proxy based architecture or any with mitigation throughput of 20Gbps.	In order to protect DDoS attack, it should always be dedicated appliance (Not part of any stateful appliance). Suggested Clause: 1. The proposed solution should have dedicated DDoS protection device (NOT be a part of Application Delivery Controller, Router, UTM, Proxy based architecture or any statefull appliance with mitigation throughput of 20Gbps.	May be read as: 1. The proposed solution should have dedicated DDoS protection device (NOT be a part of Application Delivery Controller, Router, UTM, Proxy based architecture or any statefull appliance) with mitigation throughput of 20Gbps.
105	(xv) DDoS (Hardware Appliance)	2. Throughput & H/w	1. "DDoS Flood Attack Prevention Rate: 30MPPS (min) 2. Legitimate throughput handling: 20Gbps (min) 6. The appliance should have dedicated 1 x 1G RJ45 Management Port and RJ45 Console Port."	Legitimate throughput & attack prevention rate is not inline with the mitigation throughput. There should be redundant MNG port as it is the only opion through which this appliance can be managed. Solution should not be oversized, it will add un-necessary cost to the government without any requirement. Suggested Clause: 1. "DDoS Flood Attack Prevention Rate: 12MPPS (min) 2. Legitimate throughput handling: 5Gbps (min) 6. The appliance should have dedicated 2 x 1G RJ45 Management Port and RJ45 Console Port." Request to update the clause as suggested below for suitable positioning. " 1. DDoS Flood Attack Prevention Rate: 25MPPS or more"	No Change.

106	(xv) DDoS (Hardware Appliance)	2. Throughput & H/w	4. Inspection Ports supported : 4 x 10G SFP+ from day-1 with inbuilt hardware and software Bypass. Option for additional 4 x 10G SFP+ for future use with inbuilt hardware and software Bypass	Bypass capability is not avaible with any leading OEM. Kindly allow bypass capablity with external bypass switch. **Desired revise clause for participation" 4. Inspection Ports supported : 4 x 10G SFP+ from day-1 with inbuilt hardware and software Bypass. Option for additional 4 x 10G SFP+ for future use with inbuilt hardware and software Bypass. The Solution must support Bypass capability in-built or through external hardware."**	May be read as: 4. Inspection Ports supported : 4 x 10G SFP+ from day-1 with inbuilt hardware and software Bypass. Option for additional 4 x 10G SFP+ for future use with inbuilt hardware and software Bypass. The Solution must support Bypass capability in-built or through external hardware. Failure of device should not affect traffic, solution has to be deployed in HA or auto-bypass mode and all the necessary hardware has to be supplied from day one
107	(xv) DDoS (Hardware Appliance)	3. Configuration and deployment mode	3. The Solution must have 50K SSL TPS for RSA 2K key, 35K SSL TPS for ECDSA P25 and L7 RPS should be 7 Million and L4 CPS should be 2.5 Million.	Dedicated SSL solution has already been asked as a separate solution, same should not be aprt of DDoS. Suggested Clause: 3. Delete the clause Ask Layer 7 and Layer 4 RPS and CPS at very high side and Please change it for F5 Participation. Please consider Leading OEM's hardware datasheet for L7 and L4 connections per second. Desired revise clause for participation" 3. The Solution must have 50K SSL TPS for RSA 2K key, 35K SSL TPS for ECDSA P25 and L7 RPS should be 2.5 Million and L4 CPS should be 1 Million.	No Change.
108	(xv) DDoS (Hardware Appliance)	4. Attack protection	2. The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL handshake attack 7. The solution should protect HTTP & HTTPS based attacks: HTTP GET Flood, HTTP POST Flood, HTTP Slowloris, HTTP Slow POST, HTTP URL monitor, SSL Handshake, SSL Renegotiation.	Dedicated SSL solution has already been asked as a separate solution, sam should not be aprt of DDoS. Suggested Clause: 2. The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol attack 7. The solution should protect HTTP & HTTPS based attacks	No Change.
109	(xv) DDoS (Hardware Appliance)	4. Attack protection	5. The solution should protect TCP based attacks: TCP SYN Flood, TCP SYNACK Flood, TCP ACK Flood, TCP FIN/RST Flood , TCP Connection Flood ,TCP Slow Connection , TCP Abnormal Connection,TCP Fragments Flood, Defense WinNuke, TCP Error Flag.	Request to modify the clause as suggested below for a wider participation: " 5. The solution should protect TCP based attacks: TCP SYN Flood, TCP SYNACK Flood, TCP ACK Flood, TCP FIN/RST Flood , TCP Connection Flood ,TCP Slow Connection , TCP Abnormal Connection,TCP Fragments Flood, TCP Error Flag."	May be read as: 5. The solution should protect TCP based attacks: TCP SYN Flood, TCP SYNACK Flood, TCP ACK Flood, TCP FIN/RST Flood , TCP Connection Flood ,TCP Slow Connection , TCP Abnormal Connection,TCP Fragments Flood, TCP Error Flag.

110	(xv) DDoS (Hardware Appliance)	6. HA Support	1. The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, ActiveActive using VRRP.	The specification asked is as per additional license of DDoS on top of ADC. Appliance should always be dedicated appliance only. Solution should also not be oversized, it will add un-necessary cost to the government without any requirement. Suggested Clause: 1. The solution shall have built-in Cluster features Security Solution will deployed in HA with same OEM appliances. They do share syncronisation and appliance state health with properitary protocols. Kindly allow HA functionality without VRRP like you asked in SSLO appliance. Desired revise clause for participation" 1. The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active using VRRP or equivalent."	May be read as: The solution shall have built-in high availability (HA) or cluster features in Active-Active or Active-Passive mode. Failure of device should not affect traffic, solution has to be deployed in HA or auto-bypass mode and all the necessary hardware has to be supplied from day one
111	(xv) DDoS (Hardware Appliance)	7. Management	4. The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4/IPv6 traffic to IPv6/IPv4 traffic on the backend. 5. The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.	The specification asked is as per additional license of DDoS on top of ADC. Appliance should always be dedicated appliance only. Solution should also not be oversized, it will add un-necessary cost to the government without any requirement. Suggested Clause: 4. The solution should support IPv6 as well as IPv4 inspection. 5. The solution shall be able to support IPv4 & IPv6	May be read as: 4. The solution should support IPv6 as well as IPv4 inspection. 5. The solution shall be able to support IPv4 & IPv6
112	(xv) DDoS (Hardware Appliance)	7. Management	3. The solution should support IPv4 and IPv6 dual-stack without deteriorating performance.	The IPv6 Ready Logo certification will indicate that a product has successfully satisfied the strong requirements stated by the IPv6 Logo Committee. The IPv6 Ready Core Logo expands the "core IPv6 protocols" test coverage to approximately 450 tests and adds new extended test categories. It is suggested to amend the clause as "The solution should support IPv4 and IPv6 dual-stack without deteriorating performance and IPv6 ready logo certified from the day 1 and OEM should be listed vendor for ipv6 phase-2 certification"	No Change
113	(xv) DDoS (Hardware Appliance)	Addition of Clause	Addition of Clause	Since DDoS will be forefronting all the critical Networks and applications, a lot of scanning will be performed on the DDoS and for debugging purposes Hence, we request to addition of this clause "Device should have 4 TB HDD"	No Change

114	(xvi) SSL Offloader (Hardware Appliance)	2. Throughput & H/W	1. Traffic Ports: 4 x 10G SFP+ (SX Fiber incl.), 4 x 1G copper ports 2. L4 Throughput: 20 Gbps (min) 3. SSL Throughput: 10Gbps (min) 4. Concurrent Connections: 40 Million 5. HDD: 4TB HDD (min) and dual power supply. 6. The appliance should have dedicated 2x10/100/1000 Copper Ethernet (RJ45) Management Port and RJ45 Console Port.	1Gig interface will not use in DC connectivity. Kindly asked for 10gig and 40gig instead of 1gig. Asked firewall also asked with only 10gig and 40gig interface, SSLO will connect with Firewall only and leaf switches over 10gig interface only. 4TB HDD not available in OEM's customise hardware. Kindly modify for leading OEM to qualification. Desired revise clause for participation"Traffic Ports: 4 x 10G SFP+ (SX Fiber incl.), 4 x 1G copper ports or 4 x 10Gig(SX fiber incl.) and support for 40gig in future. 2. L4 Throughput: 20 Gbps (min) 3. SSL Throughput: 10Gbps (min) 4. Concurrent Connections: 40 Million 5. HDD: 1TB HDD (min) and dual power supply. 6. The appliance should have dedicated 2x10/100/1000 Copper Ethernet (RJ45) Management Port and RJ45 Console Port.." There is no specific need for two management ports, and a single management port is sufficient for device accessibility and debugging purposes, it is suggested to amend the clause as "The appliance should have dedicated 1x10/100/1000 Copper Ethernet (RJ45) Management Port and RJ45 Console Port" Log and Data will be stored on centralized management solution, the asked requirement will unneccessary add additional cost to the government without any requirement.	May be read as: 1. Traffic Ports: 4 x 10G SFP+ (SX Fiber incl.), 4 x 1G copper ports or 4 x 10Gig(SX fiber incl.) 2. L4 Throughput: 20 Gbps (min) 3. SSL Throughput: 10Gbps (min) 4. Concurrent Connections: 40 Million 5. HDD: 1 TB SSD (min) and dual power supply. 6. The appliance should have dedicated 1x10/100/1000 Copper Ethernet (RJ45) Management Port and RJ45 Console Port.
115	(xvi) SSL Offloader (Hardware Appliance)	4. RPS & CPS	1. The appliance should support L4 CPS 1.5 Million and L7 RPS 2.5 Million. 2. The solution should support a minimum 40,000 SSL TPS for RSA 2048 bit key and 28,000 SSL TPS for ECC.	SSL offloader swill be centrally amanged all SSL traffic. SSL visiblity solution should have more SSL TPS then any other solution in network. Kindly double the SSL TPS count for today and future requirement for next 5 years. Solution should also not be oversized, it will add un-necessary cost to the government without any requirement. Suggested Clause: 1. The appliance should support L4 CPS 400,000 and L7 RPS 800,000. 2. The solution should support a minimum 20,000 SSL TPS for RSA 2048 bit key and 10,000 SSL TPS for ECC.	No Change
116	(xvi) SSL Offloader (Hardware Appliance)	7. By-pass capability	1. The Solution must support Bypass capability in-built or through external hardware.	Please remove Bypass capablity from SSLO device as same is asked in HA configuration. Bypass is relevant for stateless appliance like DDoS. Asking the same on Statefull appliance is not relevant. Suggested Clause: 1. The Solution must support High Availability.	Clause removed.

117	(xvi) SSL Offloader (Hardware Appliance)	9. Traffic interception	1. The solution must have both Inbound & Outbound SSL Interception capability. 2. The solution must support before proxy interception (between Client and Proxy) 3. The solution must support SSL interception bypass based on source and/or destination, IP, SNI values, URL category.	As solution has been asked for SSL offloading, outbound inspection should not be part of solution. Suggested Clause: 1. The solution must have Inbound SSL Interception functionality. 2. Delete the clause 3. Delete the clause	No Change
118	(xvi) SSL Offloader (Hardware Appliance)	11. Webagent support	1. The solution should support Webagent to enable explicit forward proxy	As solution has been asked for SSL offloading, outbound inspection should not be part of solution. Suggested Clause: 1. Delete the clause	No Change
119	(xvi) SSL Offloader (Hardware Appliance)	Addition of Clause	Addition of Clause	Appliance/Software should be stable and reliable in nature for such critical infra like CDAC, EAL certification ensure the same. **Suggested Clause:** **Appliance/Software should be EAL2 certified.**	No Change
120	(xvi) SSL Offloader (Hardware Appliance)	Addition of Clause	Addition of Clause	The appliance should support next generation features like Virtualization with its own Hypervisor (Not any open source or third party) that can that virtualizes the Device resources—including CPU, memory, network, configuration, operating system and acceleration resources to provide complete separate environment from network/applications and management perspective. **Suggested Clause:** **The proposed appliance should have hypervisor based Virtualization feature with its own Hypervisor (Not any open source or third party) that virtualizes the Device resources—including CPU, memory, network, configuration, oerating system and acceleration resources.**	No Change
121	(xvi) SSL Offloader (Hardware Appliance)	Addition of Clause	Addition of Clause	The IPv6 Ready Logo certification will indicate that a product has successfully satisfied the strong requirements stated by the IPv6 Logo Committee. The IPv6 Ready Core Logo expands the "core IPv6 protocols" test coverage to approximately 450 tests and adds new extended test categories. It is suggested to amend the clause as "The solution should support IPv4 and IPv6 dual-stack without deteriorating performance and IPv6 ready logo certified from the day 1 and OEM should be listed vendor for ipv6 phase-2 certification"	No Change
122	(xvii) WAF (Virtual Appliance)	1. Type	1. The proposed solution should be a Virtual appliance vWAF not as add-on license Feature on ADC and NGFW.	There are leading OEM who offer WAF on top of ADC, request to consider the same. Solution should be Elastic in nature to cater current as well as future requirement without any limitation on number of instances to be deployed. Suggested Clause: 1. The proposed solution should be a Virtual appliance vWAF-Elastic Based Model with unlimited instance support.	No Change

123	(xvii) WAF (Virtual Appliance)	4. L7 Features	1. The vWAF L7 RPS should be 1.5 Million and support 12 K SSL TPS for RSA 2K key, 8K SSL TPS for ECDSA P25.	As solution has been asked as a virtual, it should also not be oversized. This will add un-necessary cost to the government without any requirement. Suggested Clause: 1. The vWAF L7 RPS should be 700,000 and support 4 K SSL TPS for RSA 2K key, 3K SSL TPS for ECDSA. Performance of vWAF will depend upon underlying hardware, virtualisation, NIC cards, HSM device etc. Kindly remove this clause as its specific to one OEM. Please clarify asked performance parameters are as per 10Gbps total throughput.?	No Change (Performance parameters are as per 10Gbps total throughput only)
124	(xvii) WAF (Virtual Appliance)	5. Modes & security model	1. The vWAF should support in-line modes- Bridge, routed, transparent mode, reverse proxy mode and out of path (TAP/SPAN).	Bridge mode is not relevant for WAF deployment as it has to perform inspection in either L2 as a transparent or L3 as a routing mode. Suggested Clause: 1. The vWAF should support in-line modes- routed, transparent mode, reverse proxy mode and out of path (TAP/SPAN).	May be read as: 1. The vWAF should support in-line modes- routed, transparent mode, reverse proxy mode and out of path (TAP/SPAN).
125	(xvii) WAF (Virtual Appliance)	6. Attack Protection	1. The vWAF should support in-line modes- Bridge, routed, transparent mode, reverse proxy mode and out of path (TAP/SPAN). 5. The WAF should support the detection of uploading web shell attacks. The detection method should be based on the content of the uploaded file, while protecting against illegal access to the web shell; The WAF should support HTTPS-based attack protection and detection of attack behavior in encrypted data packets. 6. The WAF should protect application layer and Network DOS attacks, support application layer resource consumption type denial of service attack detection and denial of service attack detection caused by malformed data and malformed protocol. 9. The WAF should support Anti-leech to prevent the attacker from using technical means to bypass other commercial enduser windows (such as advertisement) and providing services belonging to other service providers to end users on their own website. 10. The WAF should support Web AntiDefacement (WAD) function to detect and prevent the defaced web pages from being returned to the client. It should return the cached original web page to make the anti-defacement effects unnoticeable or returns a 503 error page to the client to end the service.	Bridge mode is not relevant for WAF deployment as it has to perform inspection in either L2 as a transparent or L3 as a routing mode. File ispection & Anti-Defacement should be part of dedicated like APT or other solution. DDoS has already been asked as a separate solution, asking the same on WAF will unnecessary increase overall cost without any requirement here. Anti-leech is Single OEM terminology, who is not even recognize in any leading global reports. Suggested Clause: 1. The vWAF should support in-line modes- routed, transparent mode, reverse proxy mode and out of path (TAP/SPAN). 5. The WAF should support the detection of file upload. 6. Delete the clause 9. The WAF should support Anti-leech/Brute-force attack prevention. 10. Delete the clause	No Change

126	(xvii) WAF (Virtual Appliance)	2. Throughput & Instances	1. The solution should provide elastic based model with 10Gbps aggregated throughput, there should not be any limitation on number of instances deployed. Instances of	It is the humble request to the committee to make unlimited to finite number to finalize the BOQ with quantity, it is suggested to amend the clause as "The solution should provide 10Gbps throughput and should be the option of 20 Virtual Instances with 500 Mbps throughput or 10 Virtual Instances with 1 Gbps throughput or 5 Virtual Instances of 2 Gbps throughput or 2 Virtual Instances of 5 Gbps Throughput or 1 Virtual Instances of 10 Gbps throughput" Each instance will require CPU and memory. Unlimited instance will lead to unlimited CPU and memory which will provide by customer. Please relax this clause for reputed OEM to participate. Desired revise clause for participation" 1. The solution should provide elastic based model with 10Gbps aggregated throughput or 10 instances of 1Gbps"	May be read as: 1. The solution should provide elastic based model with 10Gbps aggregated throughput, preferably with unlimited instances from a centralized licensing server. In case of limitation of number of instances, then option has to be there to create minimum 200 instances (in HA mode) with throughput options ranging from 50 Mbps to 10 Gbps in the steps of 50 Mbps. The
127	(xvii) WAF (Virtual Appliance)	7. HA support	1. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on Standard VRRP Per VIP based Active-active & active standby unit redundancy mode.	Security Solution will deployed in HA with same OEM appliances/virtual appliance. They do share syncronisation and appliance state health with properitary protocols. Kindly allow HA functionality without VRRP . **Desired revise clause for participation" 1. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on Standard VRRP or Equivalent Per VIP based Active-active & active standby unit redundancy mode."**	May be read as: 1. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on Standard VRRP or Equivalent Per VIP based Active-active & active standby unit redundancy mode.
128	(xvii) WAF (Virtual Appliance)	3. Management	The vWAF shall be able to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.	The IPv6 Ready Logo certification will indicate that a product has successfully satisfied the strong requirements stated by the IPv6 Logo Committee. The IPv6 Ready Core Logo expands the "core IPv6 protocols" test coverage to approximately 450 tests and adds new extended test categories. It is suggested to amend the clause as "The vWAF shall be able to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one. and OEM should be listed vendor for ipv6 phase-2 certification"	No Change
129	(xvii) WAF (Virtual Appliance)	Addition of Clause	Addition of Clause	Appliance/Software should be stable and reliable in nature for such critical infra like CDAC, EAL certification ensure the same. Suggested Clause: Appliance/Software should be EAL2 certified.	No Change
130	(xvii) WAF (Virtual Appliance)	Addition of Clause	Addition of Clause	The WAF shall belong to product family which minimally attains Internet Computer Security Association (ICSA) Certification it is suggested to amend the clause as "WAF should be ICSA certified."	No Change

131	(xviii) LB (Virtual Appliance)	3. Throughput	1. The solution should provide elastic based model with 10Gbps aggregated throughput, there should not be any limitation on number of instances deployed. Instances for SLB should be unlimited.	It is the humble request to the committee to make unlimited to finite number to finalize the BOQ with quantity, it is suggested to amend the clause as "The solution should provide 10Gbps throughput and should be the option of 20 Virtual Instances with 500 Mbps throughput or 10 Virtual Instances with 1 Gbps throughput or 5 Virtual Instances of 2 Gbps throughput or 2 Virtual Instances of 5 Gbps Throughput or 1 Virtual Instances of 10 Gbps throughput" Each instance will require CPU and memory. Unlimited instance will lead to unlimited CPU and memory which will provide by customer. Please relax this clause for reputed OEM to participate. Desired revise clause for participation" 1. The solution should provide elastic based model with 10Gbps aggregated throughput or 10 instances of 1Gbps"	May be read as: 1. The solution should provide elastic based model with 10Gbps aggregated throughput, preferably with unlimited instances from a centralized licensing server. In case of limitation of number of instances, then option has to be there to create minimum 200 instances (in HA mode) with throughput options ranging from 50 Mbps to 10 Gbps in the steps of 50 Mbps.
132	(xviii) LB (Virtual Appliance)	3. Throughput	2. The Appliance should support L7 RPS 1.5 Million and L4 CPS 2 Million from day 1 and support 12 K SSL TPS for RSA 2K key, 8K SSL TPS for ECDSA P25.	As solution has been asked as a virtual, it should also not be oversized. This will add un-necessary cost to the government without any requirement. Suggested Clause: 1. The vWAF L7 RPS should be 700,000 and support 4 K SSL TPS for RSA 2K key, 3K SSL TPS for ECDSA. Performance of vSLB will depend upon underlying hardware, virtualisation, NIC cards, HSM device etc. Kindly remove this clause as its specific to one OEM. Please clarify asked performance parameters are as per 10Gbps total throughput.?	No Change (Performance parameters are as per 10Gbps total throughput only)
133	(xviii) LB (Virtual Appliance)	5. HA support	1. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based standard VRRP RFC 2338 on Per VIP based Active-active & active standby unit redundancy mode for virtual instances.	Security Solution will deployed in HA with same OEM appliances/virtual appliance. They do share syncronisation and appliance state health with properitary protocols. Kindly allow HA functionality without VRRP . Desired revise clause for participation" 1. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on Standard VRRP or Equivalent Per VIP based Active-active & active standby unit redundancy mode."	May be read as: 1. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on Standard VRRP or Equivalent Per VIP based Active-active & active standby unit redundancy mode.
134	(xviii) LB (Virtual Appliance)	2. Management	6. The solution must support Single SignOn (SSO) for web based applications and web based file server access. It should also supports SAML secure application access.	SSO Authentication should be part of dedicated solution, it can't be part of LB. **Suggested Clause:** **6. The solution must support https, CLI access for management**	No Change

135	(xviii) LB (Virtual Appliance)	4. LB & GSLB feature	17. It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc	Appliance should have DNS functionality which is relevant for LB functionality, it should behave like dedicated DNS server. **Suggested Clause:** **17. It should support advance functions Authoritative name sever, DNSSEC, application load** **balancing from day one. It should be capable of handling records including A, AAAA etc**	No Change
136	(xviii) LB (Virtual Appliance)	6. Reporting, Logging & Alert	1. The appliance should have extensive reporting and logging with inbuilt tcpdump like tool and log collection functionality. The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting. 2. The solution should support XML-RPC for integration with 3rd party management and monitoring of the devices. The appliance should provide detailed logs and graphs for real time and time based statistics.	There should be dedicated centralized management for critical infra like CDAC. REST-API is industry standard, same should be considered for integration with 3rd party management and monitoring. **Suggested Clause:** **1. The solution should have extensive reporting and logging with tcpdump like tool and log collection functionality. The appliance should have SSH CLI, Direct Console, SNMP with centralized reporting.** **2. The solution should support REST-API for integration with 3rd party management and monitoring of the devices. The solution should provide detailed logs and graphs for real time and time based statistics.**	May be read as: 1. The appliance should have extensive reporting and logging with inbuilt tcpdump like tool and log collection functionality. The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting. 2. The solution should support REST-API/XML-RPC for integration with 3rd party management and monitoring of the devices. The appliance should provide detailed logs and graphs for real time and time based statistics.
137	(xviii) LB (Virtual Appliance)	2. Management	The vSLB shall be able to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one	The IPv6 Ready Logo certification will indicate that a product has successfully satisfied the strong requirements stated by the IPv6 Logo Committee. The IPv6 Ready Core Logo expands the "core IPv6 protocols" test coverage to approximately 450 tests and adds new extended test categories. It is suggested to amend the clause as "The vSLB shall be able to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one. and OEM should be listed vendor for ipv6 phase-2 certification"	No Change
138	(xviii) LB (Virtual Appliance)		New Clause Request	Appliance/Software should be stable and reliable in nature for such critical infra like CDAC, EAL certification ensure the same. **Suggested Clause:** **Appliance/Software should be EAL2 certified.**	No Change
139			DDOS, SSLO, vWAF and VSLB asked from single OEM.	Kindly clarify can multpple OEM solution accepted.	Clause removed
140		A. Schedule of Items – BoQ, Page - 24	15-16 - Solution from Single OEM	It is asked in the BoQ that the DDoS, SSL Offloader & WAF should be from single OEM. This clause limits the wider participation and also not a good for Defence in Depth approach. Request to allow individual participation from different OEM.	Clause removed
141	(xix) NG-Firewall with ATP & Deep Inspection	4. Hardware Configuratio n	4- Hardware Configuration - Memory - 128 GB or more	Not all OEM are built with same hardware architecture and some may utilise the hardware more efficiently without need for a higher memory & yet deliver the same throuput. Moreover, the solution sizing should not be dependent on the underlying hardware configuration. Request to update the clause as below for wider particiaption. "Memory - 48 GB or more"	No Change

142	(xix) NG-Firewall with ATP & Deep Inspection	6. Throughput & Performance	6- Throughput & Performance - Concurrent Session/Concurrent Connection - 30M or higher	Requested concurrent session for a NGTP throuput of 20Gbps and 600K connection/second is on a higher side. Request to consider the change as below for appropriate sizing: "Concurrent Session/Concurrent Connection - 20M or higher"	No Change
143	(xix) NG-Firewall with ATP & Deep Inspection	7. Physical Interface	7- Physical Interface - Should have Remote Lights Out Management (Separate mgmt. port) of 1 Gbps or higher RJ45 port.	We understand that it is either an LOM port or a dedicated Management port on the appliance. Also not all OEM has LOM port option in each model but a dedicated management port can be anticipated. Request to modify the clause as suggesetd below for clarity. "Should have Remote Lights Out Management or a Separate mgmt. port of 1 Gbps or higher RJ45 port."	May be read as: Physical Interface - Should have dedicated remote management port of 1 Gbps or higher RJ45 port.
146	(xix) NG-Firewall with ATP & Deep Inspection	4. Hardware Configuration	Storage Disk - 2X 400 GB or higher for inherent log storage		May be read as: 2x400 GB SSD
147	(xix) NG-Firewall with ATP & Deep Inspection	4. Hardware Configuration	Dual Hot Swappable Power Supplies	Dual Hot swappable and field replacabale power supplies	No Change
148	(xix) NG-Firewall with ATP & Deep Inspection	4. Hardware Configuration	Redundant Fans	Dual Hot swappable and field replacabale fan	No Change
150	(xix) NG-Firewall with ATP & Deep Inspection	6. Throughput & Performance	20 Gbps Real World/Prod Performance Throughput with all features enabled including ATP, Deep Packet Inspection, SSL encryption & decryption	Clarification requested do we need to factor concurrent connection and new session per second number with all firewall, deep packet inspection, application control, anti bot etc. features enabled or it is a Layer 3 firewall only UDP/TCP performance number	No Change. 20 Gbps throughput with all features enabled (all firewall, deep packet inspection, application control, anti bot etc.)
151	(xix) NG-Firewall with ATP & Deep Inspection	6. Throughput & Performance	Concurrent Session/Concurrent Connection - 15M or higher		
152	(xix) NG-Firewall with ATP & Deep Inspection	6. Throughput & Performance	New session/Connection per second - 550K		
153	(xix) NG-Firewall with ATP & Deep Inspection	8. VPN	Number of IPSec VPN Peers supported (Site to Site) - 10K	Number of IPSec VPN Peers supported (Site to Site) - 1K	May be read as: Number of IPSec VPN Peers supported (Site to Site) - 5K All VPN Client licenses has to be included for the requirement mentioned from day one. MFA authetication licenses / tokens have to be
154	(xix) NG-Firewall with ATP & Deep Inspection		Number of IPSec VPN Peers supported (Client to Site) – 10K		

155	(xix) NG-Firewall with ATP & Deep Inspection	SSL VPN Peers supported (Client to Site) – 2K		supplied for the requirement mentioned from day one.

Queries related to Eligibility Criteria				
1	GEM bid document	Bid to RA enabled	We request to you please allow RA as it will help bidders to provide the best cost to CDAC.	Bid to RA was not enabled during bid initiation, hence GeM Portal does not allow the modification
2	GEM bid document	MII Purchase Preference	We request to you please allow MII preference as NO, as the solution asked in the bid document is not fully available with Make in India Components as couple of Major components asked in the bid, are Named Softwares which are must for solution, HCI and Cloud solutions are also not manufactured in India, Similarly storage asked in the bid also not manufacured in India , hence bidder will not be able to achieve 51% components of bid as MII, hence it may lead to a incomplete solution. **Please refer ANNEXURE-I-TECHNICAL BID SUMMARY document mentioned on 114/146 where Country of Origin and country of Manufacurer and sipment country is to be mentioned by the bidder.**	MII exemption cannot be granted. However, Class II bidders are eligible to participate, as the bid is not reserved for Class I bidders,
3	Page no 4/146 Pre-Qualification Criteria	Bidder should have executed similar turnkey projects (Data Centre IT Infrastructure installations, maintenance and support of complete Cloud Solution of not less than 20 Nodes/SDN Solution with 100Gbps backbone/Security Solution for a production throughput of minimum 10 Gbps.) with Central/State Governments Ministries/ Departments/PSUs/Autonomous Bodies during the last 5 Financial Years and current Financial year i.e FY 2018-19, 2019-20, 2020-21, 2021-22, 2022-23 & 2023-24 as follows; i) Single similar turnkey project work order/contract valuing Rs.36 Cr. (or) ii) Two similar turnkey project work orders/contracts valuing Rs.22.50 Cr. (or) iii) Three similar turnkey project work orders/contracts valuing Rs.18 Cr. Note: the project should be completed in all respects and ongoing projects shall not be considered.	We urge you to modify the clause for maximum participation i) Single similar turnkey project work order/contract valuing Rs. 15 Cr. (or) ii) Two similar turnkey project work orders/contracts valuing Rs.10 Cr. (or) iii) Three similar turnkey project work orders/contracts valuing Rs.5 Cr. Note: the project should be completed in all respects and ongoing projects where work is completed more than 70% can also be considered.	Criteria remains unchanged
4	Page no 4/146 Pre-Qualification Criteria	Minimum 2 OEM Certified resources on the direct job role of the bidder in each of the following areas; (a) Cloud solution (b) SDN Solution (c) Security Solution	We request to you to modify the clause to following Minimum 2 OEM Certified resources on the direct job role of the bidder in each of the following areas; (a) Cloud solution (b) SDN / SDWAN Solution (c) Security Solution	Criteria remains unchanged

5	Page no 4/146 Pre-Qualification Criteria	The undertakings from the Principal Manufacturers (OEMs) of equipment / items offered.	Please clarify that Prinicipal Manufacturers (OEMs) of equipmennt / item offered is required for all the components or it is specific to mentioned products in - A. Schedule of Requirement – Specification Compliance Sheet of speicific components mentioned on page no 26/146 to page no 113/146.	OEM Authorization is required for all the components offered as part of the solution
6	Page no 116/146 ANNEXURE-II-Delivery and Payment Schedule	Delivery and Payment Schedule	We request to you please modify the delivery schedule to minimum 10 weeks as delivery of HCI, Networking items, Routers and Storage is not practically fesaible in 4 weeks due to OEM dependencies and shipment of these items are dependent to countries who meet LAND & Border clause of Central Government notification.	Delivery schedule was fixed, as per the project requirements. Hence, remain unchanged
7	Page no 7/146 Technical Scoring Criteria	Each similar Turnkey projects valuing Rs.18 Cr to 22.50 Cr will get 4 marks.	We request to please modify the Project value from Rs.18 Cr to 22.50 Cr to Rs.5 Cr to Rs.10 Cr will get 4 marks	Criteria remains unchanged
8		Each similar Turnkey projects valuing more than Rs.22.50 Cr and upto 36 Cr will get 6 marks.	We request to please modify the Project value from Rs.22.50 Cr and upto 36 Cr to Rs.10 Cr to Rs.15 Cr will get 6 marks	Criteria remains unchanged
9		Each similar Turnkey projects valuing more than Rs.36 Cr will get 12 marks.	We request to please modify the Project value from Rs.36 Cr to Rs.15 Cr will get 12 marks	Criteria remains unchanged
10	Page no 7/146 Technical Scoring Criteria	PMP certified resources on the direct job role of the bidder. (2 marks for each resources and Max. 10 Marks)	We request to you kindly consider other certifcates also apart from PMP such as Certified ScrumMaster (CSM), Certified Associate in Project Management (CAPM), Project Management Professional from the International Project Management Association (IPMA), PRINCE2 Foundation (PRINCE2 Practioner), and Certified Project Manager (CPM)	Criteria remains unchanged
11	Schedule of Requirement – Specification Compliance Sheet. Page no 26/146	1)Direct installation by OEM Professional as per the Scope of Work mentioned in the document	We request to you kindly allow bidder to do the installation as SI also have the skills to deliver the solutions.	Criteria remains unchanged
12	Page no. 6, Technical Bid: A. Pre-Qualification Criteria:	Bidder should have executed similar turnkey projects (Data Centre IT Infrastructure installations, maintenance and support of complete Cloud Solution of not less than 20 Nodes/SDN Solution with 100Gbps backbone/Security Solution for a production throughput of minimum 10 Gbps.) with Central/State Governments Ministries/Departments/PSUs/Autonomous Bodies during the last 5 Financial Years and current Financial year i.e FY 2018-19, 2019-20, 2020-21, 2021-22, 2022-23 & 2023-24 as follows; i) Single similar turnkey project work order/contract valuing Rs.36 Cr. (or) ii) Two similar turnkey project work orders/contracts valuing Rs.22.50 Cr. (or) iii) Three similar turnkey project work orders/contracts valuing Rs.18 Cr.	Please clarify if you consider any specific turnkey project, such as an SDN solution or Server/HCI with networking switches or security with netowrking solution or cloud solution or a project that includes all these components.	Definition of Similar turnkey project is provided, and the same only will be considered

13	Page no.11, SECTION II: GENERAL CONDITIONS OF CONTRACT (GCC), 2. Delivery Period:	The entire supplies of items covered in this bid must be Supplied, Installed and Commissioned along with the final acceptance testing within 8 weeks from the date of placement of order. The detailed delivery and payment schedule is provided in Annexure - II. Bidders are required to comply with schedule of delivery, installation and commissioning in accordance to the proposed schedule.	The minimum product delivery time is 8-12 weeks, while the delivery time for networking equipment is 12-20 weeks. I kindly request you to consider increasing the overall delivery time to 25-30 weeks instead of the initial 8 weeks.	Delivery schedule was fixed, as per the project requirements. Hence, remain unchanged
14	Page No. 15, Security Deposit	14.1 Within 15 days of placing the order through GeM portal, the successful bidder needs to submit 5% of total contract value as "Security deposit" in the form of FD Receipt in favour of CDAC, Hyderabad /Bank Guarantee (including e-BG) from a scheduled Bank/ Online Payment i.e., NEFT, RTGS upon award of contract towards performance (Validity of Security Deposit should be 1 Year Plus Additional 3 Months). 14.2 The security deposit shall be refunded after successfully completing the project and receipt of 10% Performance Bank Guarantee towards warranty period of 5 Years and 60 days post project completion. In case of any breach of contract, the successful vendor shall be blacklisted by C-DAC, Hyderabad under intimation to all C-DAC Centres. Further, the Security Deposit shall be forfeited towards such defaults including claim additional damages, if any.	Please describe	Supplier has to submit Security Deposit of 5% of the Order value (in the form of FD or BG which shall be valid for 15 months) within 15 days of Award of Contract. The same shall be returned back, upon receitp of 10% PBG submitted upon completion of all project committments - while submission of Final Invoice
15	Pre-Qualification Criteria/ Page No-5; Clause No-4	Bidder should have executed similar turnkey projects (Data Centre IT Infrastructure installations, maintenance and support of complete Cloud Solution of not less than 20 Nodes/SDN Solution with 100Gbps backbone/Security Solution for a production throughput of minimum 10 Gbps.) with Central/State Governments Ministries/ Departments/ PSUs/Autonomous Bodies during the last 5 Financial Years and current Financial year i.e FY 2018-19, 2019-20, 2020-21, 2021-22, 2022- 23 & 2023-24 as follows; i) Single similar turnkey project work order/contract valuing Rs.36 Cr. (or) ii) Two similar turnkey project work orders/contracts valuing Rs.22.50 Cr. (or) iii) Three similar turnkey project work orders/ contracts valuing Rs.18 Cr. Note: the project should be completed in all respects and ongoing projects shall not be considered.	We would like to apprise you that the contract duration of most of the large IT system integration projects are generally 5 years which includes operations and maintenance. Hence, we request you to kindly amend this clause as: 1. The project should be completed in all respects and ongoing projects which are under Operation and Maintenace phase or have achieved the Go-Live status shall be considered. 2. We also request you to please elborate the detailed meaning of Security solutions of 10 Gbps.	Definition of Similar turnkey project is provided, and the same only will be considered

16	Pre-Qualification Criteria/ Page No-6; Clause No-5	An EMD (Earnest Money Deposit) of Rs. 1.35 Crores in the form of a Bank Guarantee from a Scheduled Commercial Bank valid for 180 days from date of opening of bid or deposit of amount in online mode into CDAC's Bank account.	As per GeM GTC, bidders having turnover of more than INR 500 Crore in any of the last 3 completed Financial Years are exempted from furnishing EMD on GeM Portal. Kindly confirm, exemption from EMD on this criteria is allowed for this bid.	In case of claiming exemption from submission of EMD, the copy of valid exemption document must be submitted.
17	SECTION II: GENERAL CONDITIONS OF CONTRACT (GCC)/Page No-15; Clause No. 14	14.2 The security deposit shall be refunded after successfully completing the project and receipt of 10% Performance Bank Guarantee towards warranty period of 5 Years and 60 days post project completion. In case of any breach of contract, the successful vendor shall be blacklisted by C-DAC, Hyderabad under intimation to all C-DAC Centres. Further, the Security Deposit shall be forfeited towards such defaults including claim additional damages, if any.	We request you to kindly amend this clause as: 14.2 The security deposit shall be refunded after successfully completing the project and receipt of ~~10%~~ 5% Performance Bank Guarantee towards warranty period of 5 Years and 60 days post project completion. In case of any breach of contract, the successful vendor shall be blacklisted by C-DAC, Hyderabad under intimation to all C-DAC Centres. Further, the Security Deposit shall be forfeited towards such defaults including claim additional damages, if any.	Criteria remains unchanged
18	SECTION III: SPECIAL CONDITIONS OF CONTRACT (SCC)/ Page No-19; Clause No.: 7. Payments	1. 70% of the value of the delivered material will be released within 4 weeks from date of delivery, and acceptance by CDAC. All the necessary/required documents related to the material and Invoices are to be submitted with the material. Software License shall be generated in the name of CDAC, Hyderabad or CDAC, Noida respectively; as per the details provided in Schedule of Requirements 2. 30% of the overall contract value will be released after the following activities; I. The overall solution is accepted, after successful installation & integration at Hyderabad & Noida Centre as per approved Architecture. II. Proper hand over of working solution. The 5 years warranty period will commence from the date of handover. III. Submission of 10% PBG towards 5 years warranty period.	Since, being a System Integrator we have to make the upfront payment to OEM, which will increase the total cost of the project. Hence, we request you to kindly amend this clause as: 1. ~~70%~~ 80% of the value of the delivered material will be released within 4 weeks from date of delivery, and acceptance by CDAC. All the necessary/required documents related to the material and Invoices are to be submitted with the material. Software License shall be generated in the name of CDAC, Hyderabad or CDAC, Noida respectively; as per the details provided in Schedule of Requirements. 2. ~~30%~~ 20% of the overall contract value will be released after the following activities; I. The overall solution is accepted, after successful installation & integration at Hyderabad & Noida Centre as per approved Architecture. II. Proper hand over of working solution. The 5 years warranty period will commence from the date of handover. III. Submission of ~~10%~~ 5% PBG towards 5 years warranty period.	Criteria remains unchanged
19	SECTION III: SPECIAL CONDITIONS OF CONTRACT (SCC)/ Page No-19; Clause No.: 8. Penalty for delayed Delivery /Services	8.1. In case, the supplier fails to complete any part of scope of the work (i.e. delivery, inspection, installation, commissioning, acceptance and training) or part thereof within the period as stipulated in the order, C-DAC reserves the right to recover from the supplier, as agreed liquidated damages and not by way of penalty, a sum of 0.5% of the price of total order value for each week or parts thereof, of the delay, subject to a maximum of 10% of basic contract value without taxes.	We request you to kindly amend this clause as: In case, the supplier fails to complete any part of scope of the work (i.e. delivery, inspection, installation, commissioning, acceptance and training) or part thereof within the period as stipulated in the order, C-DAC reserves the right to recover from the supplier, as agreed liquidated damages and not by way of penalty, a sum of 0.5% of the price of total order value for each week or parts thereof, of the delay, subject to a maximum of ~~10%~~ 5% of ~~basic contract~~ value of undelivered items/materials without taxes.	Criteria remains unchanged

20	Pre-Qualification Criteria (Page 5)	Bidder should have executed similar turnkey projects (Data Centre IT Infrastructure installations, maintenance and support of complete Cloud Solution of not less than 20 Nodes/SDN Solution with 100Gbps backbone/Security Solution for a production throughput of minimum 10 Gbps.) with Central/State Governments Ministries/Departments/PSUs/Autonomous Bodies during the last 5 Financial Years and current Financial year i.e FY 2018-19, 2019-20, 2020-21, 2021-22, 2022-23 & 2023-24 as follows; i) Single similar turnkey project work order/contract valuing Rs.36 Cr. (or) ii) Two similar turnkey project work orders/contracts valuing Rs.22.50 Cr. (or) iii) Three similar turnkey project work orders/contracts valuing Rs.18 Cr.	Request to share more details on below points:- 1.Cloud Solution of not less than 20 Nodes – We have executed a turnkey project of Datacenter (Order value more than 36 Cr) in which we have deployed servers or no. of instance which is more than 20. Kindly confirm whether such project will be considered as qualified project against the asked PQ in RFP ? 2.Security Solution for a production throughput of minimum 10 Gbps – We have executed a turnkey project of Datacenter (Order value more than 36 Cr) in which we have deployed a security solution like firewall or WAF or similar technology with throughput of more than 10 Gbps. Kindly confirm whether such project will be considered as qualified project against the asked PQ in RFP ? Or For wider participation, request to amend clause as below: Bidder should have executed similar turnkey projects (Data Centre IT Infrastructure installations, maintenance and support) with Central/State Governments Ministries/Departments/PSUs/Autonomous Bodies during the last 5 Financial Years and current Financial year i.e FY 2018-19, 2019-20, 2020-21, 2021-22, 2022-23 & 2023-24 as follows; i) Single similar turnkey project work order/contract valuing Rs.36 Cr. (or)	Definition of Similar turnkey project is provided, and the same only will be considered
21	Pre-Qualification Criteria (Page 6)	Minimum 2 OEM Certified resources on the direct job role of the bidder in each of the following areas: (a) Cloud solution (b) SDN Solution (c) Security Solution	Kindly allow 2 OEM certified resources on the direct job role of the bidder in any one of the mentioned areas.	Criteria remains unchanged
22	GENERAL CONDITIONS OF CONTRACT (GCC) (Page 11)	Delivery Period: The entire supplies of items covered in this bid must be Supplied, Installed and Commissioned along with the final acceptance testing within 8 weeks from the date of placement of order. The detailed delivery and payment schedule is provided in Annexure - II. Bidders are required to comply with schedule of delivery, installation and commissioning in accordance to the proposed schedule.	Looking on the complexity and dependencies on respective OEM for this project, request to consider 24 weeks as delivery period.	Criteria remains unchanged

ADDENDUM - SDN Solution Requirement

Gem Bid No: GEM/2024/B/4508521

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Definition	1. Proposed fabric must be the Clos network topology architecture defined using Spine, Leaf switches with VXLAN overlay and EVPN standards. 2. Fabric should have following functionalities to be achieved: a. Flexibility: Should allow workload mobility anywhere in the DC, across the Data Centre sites b. Resiliency: The proposed fabric should be able to sustain multiple link and device (Leaf & Spine), Controller failures c. Performance: The proposed fabric should be able to use full cross- sectional bandwidth (any-to-any) across all provisioned uplink ports using equal cost multi-pathing. d. Operations: Solution should provide flow analytics using hop by hop latency and packet drop info for specific flows, which helps identify, locate and root-cause data path issues across fabric architecture. e. Multi-Data Center design: The proposed architecture should provide a single pane for provisioning, monitoring, and management to deploy stretched policies across multiple Data Centers. f. All relevant licenses for all the features and scale should be quoted along with switch and all these licenses and features should be available from Day 1. 3. The leaf-spine network fabric must be capable to provide latest network virtualization technologies to provide seamless movement of any type of user across the network. 4. Leaf spine fabric must have fully distributed architecture without any centralized data plane, control plane and management plane processing on single device.		

ADDENDUM - SDN Solution Requirement

Gem Bid No: GEM/2024/B/4508521

		5. The leaf-spine fabric must support distributed anycast gateway, Active-active EVPN multihoming		
2.	Hardware and Interface Requirement	1. Leaf switches to Spine connectivity should be through uplink port using line rate of 100 Gbps or better 2. All switches including Spine and leafs should be of line rate including access ports and uplink ports. All the interfaces should be non-blocking. 3. Fabric should support scale up and scale out without any service disruption. 4. Fabric must support minimum of 02 leaf switches 5. Fabric must support minimum of 02 spine switches and scale up to 06 spine switches without any design change.		
3.	Fabric General features	1. Fabric must support various Hypervisor encapsulation including VXLAN and VLAN natively without any additional hardware / software or design change. 2. Fabric must support VXLAN Switching/Bridging and VXLAN Routing. 3. Fabric must integrate with different Hypervisor Managers viz. Vmware vCenter, Kubernetes, Redhat Openshift and manage virtualise networking from the single pane of Glass - Fabric Controller/SDN Controller for visibility of VM/Container at the controller level. 4. Fabric must integrate with all proposed L4 - L7 Physical and virtual appliances using single pane of glass i.e. Fabric Controller or SDN Controller. 5. Fabric must provide deeper visibility in terms of latency and packet drops between any two endpoints on the fabric. 6. Solution should provide L2 & L3 extension across multiple sites/ Data Centres. 7. Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless/stateful distributed firewall or rule / flow based filtering device.		
4.	Fabric Security Features	1. Fabric must have zero trust policy model for directly connected systems or hosts in order to protect against any kind of attacks like Unauthorized Access, Man - in - the - middle –		

ADDENDUM - SDN Solution Requirement

Gem Bid No: GEM/2024/B/4508521

		attack, Replay Attack, Denial of Service and to protect against Data exfiltration. 2. Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP and External AD. 3. Fabric /SDN controller should support micro-segmentation rules and policies for workloads connected to DC fabric for east-west traffic. It must also support micro-segmentation based on VM attributes / IP based zoning. 4. Fabric must support Micro Segmentation for the Virtualized and Non - Virtualized environment (Bare metal and Container). 5. Fabric must act as a State-less/stateful distributed firewall or rule / flow based filtering device with the logging capability. 6. Fabric must be capable of inserting physical and virtual L4 - L7 (FW, LB, IPS) services dynamically between multiple segment using policy-based traffic redirect. 7. The solution should provide visibility of bugs and CVEs that are impacting the installed network devices. It should also show deviation from provisioned config and image as part of the compliance. 8.		
5.	Cloud Ready & Integration with proposed cloud solution	1. Fabric architecture must support seamless network and security extension to the proposed cloud solution, multiple cloud as well. Centralized controller is able to provide seamless connectivity within proposed cloud solution, across clouds and on premise to cloud. 2. Centralized controller must provide traffic segmentation within proposed cloud solution, across clouds and On premise DC as well. There should be seamless extension of policy / segment in case workload movements between clouds or on premise to cloud 3. Centralized controller must provide complete network visibility into proposed cloud environment. 4. The SDN controller has to be integrated with the proposed cloud solution and all the required features of the SDN controller has to be demonstrated up on integration with the cloud solution. 5. The solution should support user definable work flows to carry out multiple network-wide changes		

ADDENDUM - SDN Solution Requirement

Gem Bid No: GEM/2024/B/4508521

		with Support for automated execution and conditional checks. 6.		
6.	Fabric Management	1. Fabric must provide Centralized Management Appliance or SDN Controller - Single pane of glass for managing, monitoring and provisioning the entire Fabric within Data Centre & across all Data Centers. 2. The solution should have capability for automated topology discovery 3. Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralized Management appliance or SDN Controller. 4. Centralized management appliance or SDN Controller should not participate in Data plane and control plane traffic path of the fabric and a network device must continue to forward packet in case it loses connectivity to the manager. 5. Centralized management appliance or SDN Controller must provide Anomaly and Advisory reports for compliance and audit. 6. Solution should be able to store historical data to provide anomalies and trending information of each resource (environment, configuration & operational) and graphical representation of parameters to help debug. 7. Solution should provide an automated mechanism to find configuration deviations, security risks & non-compliances against segmentation rules by assessing current configuration, network security policies and generate alert for any deviation to provide assurance. 8. Management and monitoring of the Data Center Network must be provided through GUI centrally 9. All network Devices including leaf switches, Spine Switch should be automatically provisioned minimizing human effort and human errors with network wide configuration deployment. 10. The solution should provide scale out capability with centralized management to receive SPAN traffic on 100G ports directly connected from each leaf switch, do packet operations like header (VXLAN, GRE, ERSPAN, GENEVE) striping, packet truncation, PTP timestamping, masking of confidential data within packet through regex and packet deduplication before the traffic is sent out and load-balanced to other tools like NDR, SIEM,		

ADDENDUM - SDN Solution Requirement

Gem Bid No: GEM/2024/B/4508521

		etc. All configurations of the solution should be available through GUI. 11. All the network devices and solution components should be manageable and monitored through GUI completely.		
7.	Network Visibility & Analysis	1. Solution should provide network visibility and historical analysis between any two timeframes to identify any issues and changes including user information 2. The solution should provide pre-change analysis of the configuration to highlight any challenges and issues before pushing the configuration within the fabric to reduce the risk of network failures and human errors for a robust change management. 3. Solution should provide instant visibility into any relevant and applicable bugs and security advisories for running hardware and configuration. 4. Solution should provide recommendations on software update & best practices based on installed platforms and running configuration in network practices based on installed platforms and running configuration in network. 5. Centralized management appliance or SDN Controller must communicate to south bound devices using open standard protocols or using Device APIs. 6. The solution should provide real-time monitoring of various parameter of the network device using real-time state streaming telemetry or better technology. 7. The solution should provide real-time monitoring of various parameter of the network device using real-time state streaming telemetry or better technology. 8. The streaming telemetry data from all network devices should be available for historical analysis of past events in time-series format for 2 or more months. 9. The solution is expected to provide real-time monitoring of various network device parameters like CPU, Memory, interface stats (traffic counter, error, discard), MAC table, ARP table, IPv6 ND table, RIB, BGP, capacity parameters (TCAM), file system storage parameters, VXLAN, running config, traffic flow (OpenFLOW / sflow / IPFIX / Netflow), LLDP, buffer utilization per interface, LAG / MLAG /		

ADDENDUM - SDN Solution Requirement

Gem Bid No: GEM/2024/B/4508521

		LACP Stats, Switch environment stats (FAN, Temperature, Power Supply), etc. with streaming telemetry. 10. The solution should be capable to show in real-time congestion hotspots in the network with buffer level utilization info from the network devices. 11. The solution should show real-time & historical analysis of network traffic flows. It should provide analysis of network traffic patterns over months, days, or minutes by drilling down to an individual IP and application. Should support ingestion of at least 5K flows per second. 12. The analytics solution should be capable of performing proactive (machine learning based) analysis and provide anomaly detection with auto baselining and alerts on traffic flow parameters 13. Notification and device events should be available to operator in a manner that are easy to correlate by directly showing them over physical topology for various device and link level metrics. 14. The solution should capture meta data packets like ICMP, ARP, DNS, DHCP, TCP Syn/syn-ack packets to provides deeper analytics, like identifying rogue DHCP/DNS servers, IP/MAC spoofing, new endpoints, most used domain names, etc. 15.		
8.	Redundancy & Availability	1. Centralized management appliance or SDN Controller must run in "N +1" redundancy to provide availability as well as to function during a split-brain scenario. 2. In the event of failure of all Centralised management appliances or SDN Controllers, the fabric must function with the current configuration and without any performance degradation. 3. Centralized management appliance or SDN Controller must provide real-time device inventory and network topology of the fabric. 4. All the infrastructure including hardware and licenses required by fabric controllers to support the listed features and scale, should be provided by the bidder. 5. All the features mentioned in this document shall be available from Day 1. Hardware, Solution Software and licenses should be supplied from Day 1 to support these features. 6. Data Center Network must be fully resilient in all		

ADDENDUM - SDN Solution Requirement

Gem Bid No: GEM/2024/B/4508521

		aspects. It must continue to perform packet forwarding on any single link failure. A single switch failure should not impact forwarding for hosts connected to other switches. The architecture should provide two or more equal cost forwarding paths from switches to core. 7. The solution should provide centralized dashboard to upgrade all the network devices with ease without incurring traffic downtime in network. 8. Solution should provide simplified and quick way of network wide rollback for device configuration and images to revert back changes if required. 9. Any additional hardware, if required to run the dashboard/GUI must be part of the bid and must be provided in HA at both DC and DR		
9.	General requirements, warranty and support	1. Manufacturer Authorization is Required 2. All the required network switches, software, license and support components should be factored as per the specification and should be from same OEM from Day 1. Specifications mentioned are minimum required, OEM/Bidder can quote higher models/specifications. 3. OEM(s) professional Services have to perform complete plan, design, implementation and validation of all components of the solution, OEM professional Services personnel should be on OEM Payroll only. Part Number of the same need to be shown in Technical Bid 4. The proposed solution OEM(s) should have a registered office in India and an India local Technical Assistance center (with an India local number to reach the TAC). 5. TAC support for (Routers, Spine, Leaf, Management Core & Management/OOB Switch) solution must be directly from single OEM. OEM should have 24x7 TAC available over email and Phone. 6. Bidder should submit fully complied solution, any deviation will result in bid rejection and Intentional wrong compliance claims will result in blacklisting of OEM & Bidder for next 3 years 7. The OEM professional services should also provide knowledge transfer and handover training for minimum 2 weeks and OEM certification for 5 members 8. All Quoted Models / Products (Data Center Network Management and Visibility Solution, Routers, Spine, Leaf, Management Core &		

ADDENDUM - SDN Solution Requirement

Gem Bid No: GEM/2024/B/4508521

		Management/OOB Switch) should have support life of 7 years minimum from the Date of installation sign off, same need to be confirmed in signed MAF. 9. OEM/Bidder should have quoted required hardware/VM's/appliance to deploy Data Center Network Management and Visibility Solution in HA. 10. Minimum Qty Required - 1 Solution at DC in HA & 1 Solution at DR in HA		