Nepal Electricity Authority
(A Government of Nepal Undertaking)
Finance Directorate
INSTITUTIONAL STRENGTHENING PROJECT

नेपाल विद्युत प्राधिकरण
स्थापित २०४२
ESTD. 1985
NEPAL ELECTRICITY AUTHORITY

Ref. No: 2078/79/ - 80

Date: Thursday 26 May 2022

To:
All prospective bidders,

Subject: Issuance of Clarification-6

OCB No. and Title: ICB/FD/EGMPAF/RMS-078/79-02 Procurement of Information Technology Products and Services "Supply and Installation of Revenue Management System (RMS)"

Project Title: Electricity Grid Modernization Project - Additional Financing

Dear Sir/Madam,

With reference to the bid published on 18 February 2022, we would like to inform all our prospective bidders about the issuance of Clarification-6 according to the ITB clause 7.1 of the bidding document.

Kindly acknowledge the receipt of the same at the project office.

Best regards,

Chandha Neupane

Chandha Neupane,
(Project Director)

OCB No. and Title:

ICB/FD/EGMPAF/RMS-078/79-02 Procurement of Information Technology Products and Services "Supply and Installation of Revenue Management System (RMS)"

Project Title:

Electricity Grid Modernization Project - Additional Financing

Clarification -6

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
1	Vol-II 3.2.3 Customer Care centre	6-240	Customer care center 1. VM base License for ACD, 2. IVR+ Dialler+ Recording+ reporting, 3. PRI- Gateway, 4. Agent License, 5. Supervisor License, 6. Server with OS for ACD + IVR, 7. Workstations and PCs – 4 for each province – with soft calling and headphones, 8. Network devices (firewall +Switch), 9. Multi-function printer, 10. Furniture, 11. IP Phone	Customer Care Center (CCC) in Schedule 1: VM base license for ACD (2 licenses at one location), which means to deploy 2 servers with ACD+IVR operating system in one location (2 servers deployed in the central location) , right? And only ACD + IVR function need be implemented? If so, please advise in which servers shall the applications like outgoing call, online call, email, recording, report, agent map and agent desktop (workbench) etc. in Customer Care Contact Center system function requirements be deployed?	SI can deploy CCC solution on Virtual Servers if the solution doesn't support VM's then SI is responsible to provide the required infrastructure.
2	Vol-II General	6-240	Additional Queries	Who is responsible for the construction and opening of the network links in the seven locations of customer care center?	Network links will be provided by NEA.
3	Vol-II General		Additional Queries	The (CCC-software) in Schedule 1 does not contain the server quotation for IP PBX deployment, and the solution does not specify the number of IP PBX requirements. Should IP PBX be deployed on the cloud or on a server? Besides, in Schedule 1, PRI gateway belongs to CCC software, so PRI gateway must be software? Is our understanding correct? Please clarify.	SI can deploy CCC solution on Virtual Servers if the solution doesn't support VM's then SI is responsible to provide the required infrastructure.
4	Vol-II General		Additional Queries	The RMS software and hardware server resources configured according to the requirements have far exceeded the hardware-server bidding requirements. Thus do we need to configure the computing, storage, and modify the quotation list to provide quotations according to the actual needs of the RMS software?	Mentioned Quantities and Specifications are minimum requirement.
5	Vol-II General		Additional Queries	How far is the network transmission between the data center and the data recovery center? According to the distance of the link (if the data center and the data recovery center are not together), it is recommended to configure a global load in the list to ensure the resource switching of software applications? (There is no load balancing configured in the hyper-converged list)	Bandwidth between DC and DR will be provided by NEA.
6	Vol-II General		Additional Queries	Shall the data center and data recovery center hardware - server resources (computing, storage resources) be configured in consistent to meet the normal operation of the RMS software system? The requirements in the current tender list are inconsistent.	DC will have both prod and non-prod workloads and DR centre will have prod workloads only
7	Vol-II General		Additional Queries	Is it necessary to add network equipment such as core switches and routers in the data center and data recovery center? Because there are only the requirements of TOR switches in this list, if it's necessary to add, please give specific parameters and quantity requirements. In addition, according to the hyper-converged hardware configuration, two TOR switches do not meet the actual network switching requirements, thus the number of TOR switches needs to be added. Can the number of TOR switches be modified? Can the bidding list be modified? For example, what if the quantity we configure is more than that required in the bidding list?	Mentioned Quantities and Specifications are minimum requirement.

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
8	Vol-II 3.2.1.1.1 Microservice Architecture	6-205	RMS solution components must follow microservice principles to provide specific services using well defined Advanced Message Queuing Protocol (AMQP). Identify opportunities for cross-functional components or subsystems and implement them in such a way that there is an opportunity for reuse. This defines integration architectures based on the concept of a service and becomes relevant especially when there are multiple applications in an enterprise and point-to-point integration between them involves complexity.	RMS system should be built on a microservice architecture is an option or mandatory ? And it can be accept that use Monolithic Architecture?	This is the Bid Document requirement and hence it is written as 'must follow' which leaves no space for speculation of using a monolithic architecure. Bid Document cluase shall prevail.
9	Vol-II 3.2.1.1.10 Backup and Recovery	Page 6-208	Service Provider shall ensure that the data is replicated at the backup site at DR Site.	In the IT technical specification, data backup is required to be in the DR site, but this backup method is stored in certain security risks, such as the downtime of the DR site and the DC site, resulting in data loss; and the backup from the DC site to the DR site is all about network bandwidth. There are requirements and there are also cyber risks.In order to solve the above security problems, does it can be accept that using backup software and backup devices locally? Pls confirm it.	Bandwidth between DC and DR will be provided by NEA.
10	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-211	Solution should include an application and infrastructure performance management tool quoted as part of the solution to improve operations and provide deep infrastructure performance insight.	This is Vendor Specific:- Explore vRealize Operations/Tanzu Observability for application level monitoring, as well as more granular monitoring Suggestation-Solution should include infrastructure Performance monitoring as part of the solution to improve operations and provide deep infrastructure performance insight.	Solution should include either inbuilt or 3rd party integrated infrastructure Performance monitoring as part of the solution to improve operations and provide deep infrastructure performance insight.
11	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-215	HCI solution should have codeless automation native engine to create troubleshooting for alert and remediation as per policy	This is vendor Locked ,Suggest to remove this point	Bidder should provide automation engine to create troubleshooting for alert and remediation as per policy either inbuilt in HCI or 3rd party solution
12	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-217	Private Cloud Orchestrator	why we need Private cloud orchestrator , IF HCI fullfill the requirement ? Suggestation:-Remove this whole segment as to comply this we need to propose VMware Cloud Foundation (VCF) which will uplift the budget	No Change, NEA wants to deploy private cloud and this is required,
13	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-219	Firmware Code and Patch Management All patches for the complete hardware and software solution must come from a single validated source. It should be possible to apply and upgrade all software and Hardware related firmware and patches from the same GUI that is used to manage the HCI (It should not use the hardware management console for doing firmware upgrade of hardware)	This is vendor specific Suggestation :-All patches for the complete hardware and software solution must come from a validated source. It should be possible to apply and upgrade all software and Hardware related firmware and patches from the GUI.	All patches for the complete hardware and software solution must come from a validated source. It should be possible to apply and upgrade all software and Hardware related firmware and patches from the GUI.

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
14	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-209	Total usable cores: Database compute (24 core, 3.0 GHz). Latest Generation processor across Cluster Web Application & others (144 core, 2.1 GHz) 2. For DC Total useable cores: Database compute (32 core, 3.0 GHz). Latest Generation processor across Cluster Web Application & others (176 core, 2.1 GHz) Total RAM: Database Compute with 24 GB per CPU Core and for Web, Application and Other Compute with 8 GB per CPU Core DDR4 3200 MHz across Cluster For DR Total useable cores: Database compute (24 core, 3.0 GHz). Latest Generation processor across Cluster Web Application & others (144 core, 2.1 GHz). Total RAM: Database Compute with 24 GB per CPU Core and for Web, Application and Other Compute with 8 GB per CPU Core DDR4 3200 MHz across Cluster	on Esxi hypervisor vmware cluster can run oracle RAC cluster VMs	Bidder can propose their choice of Hypervisor
15	Vol-II 3.2.2.1.1Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-209	Storage: 40 TB Usable across Cluster (20% should be SSD) Note: Should be hot swappable and field replaceable. NAS Storage: 62 TB	Total all flash provided better performance across the cluster as in HCI pool of SSD is created and data is striped in blocks across the nodes in cluster	Bidder can propose all Flash, 62TB NAS should be provided in HCI
16	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-211	The solution should provide enterprise data services such as deduplication, encryption & compression without dependence on any proprietary hardware. This should be delivered in both all flash as well as hybrid solution. These functionalities should be part of the proposed solution and licensed. The proposed HCI solution should be able to create multiple logical unit (LLIN's) for storage with multiple policy for deduplication and compression across storage logical unit. The Proposed HCI solution should support Erasure Coding for archival data storage.	Erasure coding is a data saving technique and have huge performance impact as it uses higher usage of compute resources , retreival latencies increases when we use earsure coding.In addition when we use erasure coding in DC-DR set up then also WAN network traffic increases.	No Change, NEA wants to deploy private cloud and this is required,
17	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-212	Data compression, deduplication, erasure coding techniques should be available with licenses (if applicable) in the Software Defined Storage (SDS) layer for use without additional cost.	Erasure coding is a data saving technique and have huge performance impact as it uses higher usage of compute resources , retreival latencies increases when we use earsure coding.In addition when we use erasure coding in DC-DR set up then also WAN network traffic increases.	No change, NEA shall provide the required Bandwidth.
18	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-217	Central administrator must be able to manage/control the marketplace view for the tenants. Any authorised user must be able to deploy the application using the published VMs in his application marketplace.	The management software doesn't provide a marketplace view for the tenants. But can deploy EC2 instance or VMs on public Cloud.	No Change, NEA wants to deploy private cloud and this is required,
19	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-217	The solution must allow restriction of vCPU, Memory and Disk resources to each project or group of users	please confirm if customer is taking about having RBAC access controls for cpu , memory or disk	No Change, NEA wants to deploy private cloud and this is required,

chandra

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
20	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-217	The solution must provide a marketplace to allow user to consume the creation of infrastructure easily	Marketview place is part of public cloud and with cisco cloud software user can view , manage , orchestrate and automate VM/instances in cloud too.	No Change, NEA wants to deploy private cloud and this is required,
21	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-217	The software must be able to integrate with monitoring software.	There is no need to integrate with any other monitoring software as cisco FSO suite provides complete monitoring and visibility of the resources and applications consuming those resources.	As per bid document
22	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure, Software Defined Network and Cloud Orchestrator	6-217	The software must be able to integrate with application security vulnerabilities detection software	There is no need to integrate with any other with application security vulnerabilities detection software as cisco intersight basic feature natively provide security advisories , bugs, field noticely proactively	As per bid document
23	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-220	Have option for encrypted backup file	Please remove this point.	This is basic feature
24	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-220	Firewall should have minimum 40 Gbps of VPN throughput	Please revise the clause	As per bid document
25	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-220	Firewall should have 50000 site-to-site & client to site VPN Tunnels.	Please revise the clause	As per bid document
26	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-220	Firewall should have 450,000 new sessions per second	Please revise the clause	As per bid document
27	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-220	Firewall should have 8 Million concurrent sessions	Please revise the clause	As per bid document
28	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-220	The solution should have minimum 9 Gbps of NGFW throughput for Mix / production traffic	Please revise the clause	As per bid document
29	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-221	The solution should have minimum 7 Gbps of Threat Prevention throughput for Mix / production traffic	Please revise the clause	As per bid document
30	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-221	b) SMTP, SMTPS	Please remove this point	Feature required bidder can propose either inbuilt or 3rd party solution to meet the requirement.
31	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-222	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.	Please remove this point	Feature required bidder can propose either inbuilt or 3rd party solution to meet the requirement.
32	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-222	a) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies.	Please remove this point	Feature required bidder can propose either inbuilt or 3rd party solution to meet the requirement.
33	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-222	c) Shall include score-based web keyword block	Please remove this point	Feature required bidder can propose either inbuilt or 3rd party solution to meet the requirement.
34	Vol-II 3.2.3.1.6 Firewall	6-251	Firewall appliance should be supplied with at least 8x1 GE RJ45, In addition, it should have dedicated 1GE RJ-45 interfaces for Management and High Availability, 1 x USB Port. 2 Dedicated port RJ45.	Please change this point as "Firewall appliance should be supplied with at least 24x1 GE RJ45, In addition, it should have dedicated 4x 10G Ports"	As per bid document

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
35	Vol-II 3.2.3.1.6 Firewall	6-252	Firewall should support at least 35000 new sessions per second	Firewall should support at least 30000 new sessions per second with Application visibility enabled.	As per bid document
36	Vol-II 3.2.3.1.6 Firewall	6-252	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.	Please remove this point	As per bid document
37	Vol-II 3.2.3.1.6 Firewall	6-252	The proposed system should have integrated Traffic Shaping functionality.	Please change this as "The proposed system should have integrated QOS functionality."	Traffic Shaping or QoS are same.
38	Vol-II 3.2.3.1.6 Firewall	6-253	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.	Please remove this point	Feature required bidder can propose either inbuilt or 3rd party solution to meet the requirement.
39	Vol-II 3.2.3.1.6 Firewall	6-253	Should have Anti-Spam Capability to detect and block Spam Emails over IMAP, SMTP, POP3, MAPI	Please remove this point	Feature required bidder can propose either inbuilt or 3rd party solution to meet the requirement.
40	Vol-II 3.2.3.1.6 Firewall	6-254	IPS solution should have capability to protect against Denial of Service (DOS)/DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.	Please remove this point	Feature required bidder can propose either inbuilt or 3rd party solution to meet the requirement.
41	Vol-II 3.2.3.1.6 Firewall	6-254	The proposed firewall shall support 10 logical firewalls	Please remove this point	As per bid document
42	Vol-II 3.2.2.1.6 ANTI-APT	6-221	The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database.	Please remove this point	As per bid document
43	Vol-II 3.2.2.1.6 ANTI-APT	6-229	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG/GIF/BMP/WMF and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zeroday attacks	Please remove this point	As per bid document
44	Vol-II 3.2.2.1.6 ANTI-APT	6-230	The solution should protect the endpoints against advanced threats including zero- day attacks, which target application vulnerabilities that have yet to be discovered or patched.	Please remove this point	As per bid document
45	Vol-II 3.2.2.1.6 ANTI-APT	6-230	The solution should protect the endpoint by monitoring the host memory to detect and block various memory techniques like return-oriented programing, heap spraying, etc.	Please remove this point	As per bid document
46	Vol-II 3.2.2.1.6 ANTI-APT	6-230	The proposed solution shall support 8 VM and upgradable upto 14 VM in future if required.	Please remove this point	As per bid document
47	Vol-II 3.2.2.1.6 ANTI-APT	6-230	The APT appliance should be able to process minimum of 160 files/hour or 115,000 files/month (either web or mail or client or all) on VM sandboxing	Please remove this point	As per bid document
48	Vol-II 3.2.2.1.3 Internet Intrusion Prevention System	6-224	IPS should have 450,000 new sessions per second	Please share the actual requirement	This is actual requirement
49	Vol-II 3.2.2.1.3 Internet Intrusion Prevention System	6-224	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.	Please remove this point	As per bid document

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
50	Vol-II 3.2.2.1.3 Internet Intrusion Prevention System	6-224	The proposed solution should support Virtualization (IPS). Minimum 10 Virtual IPS license should be provided.	Please remove this point	As per bid document
51	Vol-II 3.2.2.1.3 Internet Intrusion Prevention System	6-225	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy lookups.	Please remove this point	Feature required bidder can propose either inbuilt or 3rd party solution to meet the requirement.
52	Vol-II 3.2.2.1.3 Internet Intrusion Prevention System	6-226	The proposed system shall support active-passive virtual clustering that uses virtual unit partitioning to send traffic for some virtual units to the primary cluster unit and traffic for other virtual units to the backup cluster units. If a failure occurs and only one cluster member continues to operate, all traffic fails over to that physical unit, like normal HA.	Please remove this point	As per bid document
53	Vol-II 3.2.2.1.4 Web Application Firewall	6-227	Appliance Should have 4-10Gig ports, 64 GB RAM and storage capability of 4 TB. Clarification 4 dated 19th April : No. of interface required are 4*10G interfaces. Interfaces should be both fiber and copper compatible. WAF appliance throughput should be minimum 30 Gbps and support 35K TPS for RSA2K and 25K TPS for ECC. It should support minimum 10 million concurrent connections and 5 million L7 RPS.	Appliance Should have : a) Traffic Ports supported : 24 x 10 GbE SFP+ (Without use of Breakout Cables, 6 X 1G Copper and 6 x 10 G SR MM from day 1), b) 32 GB RAM and scalable upto 256 GB of RAM. c)Device L4 Throughput : 30 Gbps and scalable upto 80 Gbps. d) Layer 4 connections per second: 1 M CPS e) Layer 7 requests per second: 2 M RPS f) SSL Throughput: 22 Gbps g) SSL CPS : 25K (RSA 2K Key) , 20K (ECC Key) and scalable h)The appliance should have dual power supply and dedicated 2 x 10/100/1000 Copper Ethernet Out-of-band Management Port. The Proposed solution should include Separate Management solution for centralized management and monitoring with a log retention of 365 days for forensics purpose.	As per bid document
54	Vol-II 3.2.2.1.4 Web Application Firewall	6-227	Proposed WAF should be future ready and have capability to install CentOS and Ubuntu based VNF for adapting to suture security requirements on the same appliance.	The proposed appliance should have Hypervisor(should not use open source) based Virtualization that virtualizes the device resources—including CPU, memory, network, acceleration resources, operating system and management It should NOT use Open Source/3rd party Network Functions. The Proposed Appliance should support Standalone as well as Virtualized Mode (Bidder may be asked to demonstrate the functionality). The appliance should support a minimum of 5 virtual instance from Day -1 for multi application and multi-zone deployment scalable to 32 to meet future requirements	As per bid document
55	Vol-II 3.2.2.1.4 Web Application Firewall	6-227	The solution should have license upgrade feature on same appliance to support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access/authentication to corporate resources.	Kindly Remove this Clause.	As per bid document
56	Vol-II 3.2.2.1.4 Web Application Firewall	6-227	New Clause request	OEM should be present in the "LEADER" quadrant in the Last published Gartner Report for ADC & Leader/Strong Performer quadrant of latest Forrester report for WAF. OEM should have TAC based in SAARC.	As per bid document

Chadha

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
57	Vol-II 3.2.2.1.4 Web Application Firewall	6-227	New Clause request	Proposed WAF and DDoS Should integrate with each other. It should have a unique Messaging mechanism where WAF efficiently mitigates attacks by sending attack information to DDoS located at the Network Perimeter. WAF and DDoS should be from same OEM.	As per bid document
58	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	The proposed solution should have the capability to be configured in detect as well as protect mode. The proposed appliance should be hyperconverged network function appliance should have capability to install CentOS/ Ubuntu and other open source virtual network functions and have adequate resources to ensure complete DDoS protection	The proposed solution should have the capability to be configured in detect as well as protect mode	As per bid document
59	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	Proposed appliance should have capability to install open source and 3rd party network functions for incorporating zero day features in the same appliance.	The proposed solution should prevent suspicious outbound traffic for threats and blocking malicious traffic.	As per bid document
60	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	The proposed solution must provide the ability to block bot -originated traffic according to system- supplied signatures	The proposed solution must provide the ability to block bot -originated traffic according to system-supplied signatures. Device should have atleast 5000+ pre-defined signatures and should have provision to create additional user defined signatures apart from inbuilt signatures.	As per bid document
61	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	The DDoS solution should be a dedicated hardware with dual power supply . The appliance should have 4 X 10GE SFP+ ports	Support Flood Attack Prevention Rate: upto 25 MPPS (In addition to Legitimate throughput) Attack Concurrent Sessions : Unlimited Mitigation Throughput : 20 Gbps. Legitimate Throughput : 2 Gbps scalable to 12 Gbps. Inspection Ports supported : 8 X 1G Copper and 8 x 10 G SR MM fully polulated from day and another 4 x 1G ports, 4 x 10 GbE SFP+ for future use (Without use of Breakout Cables) Latency should be less than 60 microseconds (Mentioned in publically available Datasheet) The appliance should have dual power supply and dedicated 2 x 10/100/1000 Copper Ethernet Out-of-band Management Port.	As per bid document
62	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	Devices should be proposed in high availability using standard VRRP Protocol. No proprietary protocol should be used	Devices should be proposed in high availability.	As per bid document
63	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	It shall defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Automatic Real Time protection for Zero Day attack based on Rate Variant, Rate Invariant algorithms or equivalent mechanisms without human intervention.	It shall defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Automatic Real Time protection for Zero Day attack based on Rate Variant, Rate Invariant algorithms or equivalent mechanisms without human intervention within 30 Seconds. System should have DNS Flood protection for each type of query including, A, MX, PTR, AAAA, Text, SOA, NAPTR, SRV etc.	As per bid document
64	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	New Clause Request	DDoS OEM should be present in the "LEADER" quadrant in the Latest published Forrester wave Report OR IDC Report for DDoS. DDoS OEM should have TAC based in SAARC.	As per bid document

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
65	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	New Clause Request	The proposed solution should have REAL-TIME attacker intelligence feeds from Day-1 , pertaining to a active attack sources recently involved in attacks. The feed should support real-time and ongoing validated and actionable threat intelligence from multiple sources for preemptive protection. OEM should have 24x7 (SLA defined), REAL TIME Emergency Response Services for the network facing denial-of-service (DoS) attack in order to restore network and service operational status.	As per bid document
66	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	New Clause Request	For Future Scalability, The proposed solution should support Integration with OEM Cloud based Scrubbing Centers, in case of Bandwidth Saturation attacks, using the same technology. DDoS Scrubbing Centre must be in SAARC.	As per bid document
67	Vol-II 3.2.2.1.5 Anti-DDoS	6-228	New Clause Request	Bidder should propose Separate Centralized Management & Reporting Solution from Day 1. The proposed WAF and DDoS Solution should be managed from the same Centralized Management Solution.	As per bid document
68	Vol-II 3.2.2.1.2 Internet Next Generation Firewall	6-222	High Availability	Dell Technologies having the largest HCI Portfolios as per below:-	As per bid document
69	Vol-II Database Compute (Virtualization)	6-209	Database Compute (Virtualization)	Core Based Database/Application would be very costly by license the entire Virtualization Cluster (Application 176 Core + Database 32 Core)	As per bid document
70	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure,software define Network and Cloud Orchestrator	6-209	Storage	40TB of SATA drive is definitely not recommended for mission critical application due to high failure rate (MTBF) of the drive and the performance is very very slow. **SATA drive is only recommend for Backup Storage/non critical application.	As per bid document
71	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure,software define Network and Cloud Orchestrator	6-209	NAS Storage	62TB SATA, I assume this is using for backup? We don't recommend customer to backup the HCI system within HCI system which is super high risk for customer if the HCI Datastore is down, the backup will be down too, no way to recover.	As per bid document
72	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure,software define Network and Cloud Orchestrator	6-210	Hyper Converged Solution Requirements	The solution must be able to survive single node failures and it should in no way affect/degrade the production services & usable resources to the end user application. Solution must support all the mentioned industry Leading protocols NFS, iSCSI & SMB.	As per bid document
73	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure,software define Network and Cloud Orchestrator	6-210	Hyper Converged Solution Requirements	The solution should provide enterprise data services such as deduplication, encryption & compression without dependence on any proprietary hardware. This should be delivered in both all flash as well as hybrid solution. These functionalities should be part of the proposed solution and licensed. The proposed HCI solution should be able to create multiple logical unit (LUN's) for storage with multiple policy for deduplication and compression across storage logical unit. The Proposed HCI solution should support Erasure Coding for archival data storage.	No change, NEA shall provide the required Bandwidth.

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
74	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure,software define Network and Cloud Orchestrator	6-211	Scalability	The solution should be able to scale by support of adding additional nodes to the cluster at a later point of time to handle compute, Memory & Storage requirements. Solution should support cluster expansion with zero down time. The proposed solution should support hybrid and all flash nodes in same cluster for future scalability. HCI solution must have capability to support HCI nodes with different models, different CPU Generations & Memory, Disks configurations in the same cluster without any impact on enterpriseclass storage services/functionalities	The solution should be able to scale by support of adding additional nodes to the cluster at a later point of time to handle compute, Memory & Storage requirements. Solution should support cluster expansion with zero down time.
75	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure,software define Network and Cloud Orchestrator	6-212	Hypervisor	Hypervisor should support container and openstack integration for cloud native application	As per bid document
76	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure,software define Network and Cloud Orchestrator	6-215	Networking	Recommend to remove this due to the application would only use handful of VM (not hundreds).	As per bid document
77	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure,software define Network and Cloud Orchestrator	6-217	Private Cloud Orchestrator	Recommend to remove Private Cloud Section which is not relevant to this Application and add the unneccessary cost to NEA. **Private cloud is recommend for the customer who run more than 1000 VM with multiple mix of applications. I don't see a relevant to this application design.	As per bid document
78	Vol-II 3.2.2.1.1 Hyperconverged Infrastructure,software define Network and Cloud Orchestrator	6-218	Private Cloud Database Life Cycle Management Tool	Recommend to remove Private Cloud Section which is not relevant to this Application and add the unneccessary cost to NEA.	Feature required bidder can propose either inbuilt or 3rd party solution to meet the requirement.
79	Vol-II 3.2.2.1.4 Web Application Firewall	6-227	Proposed WAF should be ICSA certified.	Recommended to delete	As per bid document
80	Vol-II 3.2.2.1.7Antivirus Solution for Servers	6-231	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
81	Vol-II 3.2.2.1.7Antivirus Solution for Servers	6-231	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	Recommended to delete	As per bid document
82	Vol-II 3.2.2.1.8Antivirus Solution for Servers	6-232	Should be able to check the reputation of the files hosted in the internet	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
83	Vol- II 3.2.2.1.9Antivirus Solution for Servers	6-232	Should be able check the reputation of the files in webmail attachments	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
84	Vol-II 3.2.2.1.10Antivirus Solution for Servers	6-232	Should be able to check the reputation of files residing in the computer	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
85	Vol-II 3.2.2.1.11Antivirus Solution for Servers	6-232	Should protect customers and servers on the network, high performance network virus scanning, and elimination.	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
86	Vol-II 3.2.2.1.12Antivirus Solution for Servers	6-232	Should provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
87	Vol-II 3.2.2.1.13Antivirus Solution for Servers	6-232	Should have smart feedback to enable feedback from the customer agents to the threat research Centers of the vendor.	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
88	Vol-II 3.2.2.1.14Antivirus Solution for Servers	6-233	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from customer IPS, customer firewall, and/or network virus logs exceed certain thresholds, signalling a possible attack	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
89	Vol-II 3.2.2.1.16Antivirus Solution for Servers	6-233	Should be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
90	Vol-II 3.2.2.1.18Antivirus Solution for Servers	6-233	System should be configured in such a way that at no case no endpoints/remote agents will be able to communicate with OEM cloud for obtaining updates through internet.	Recommended to delete	As per bid document
91	Vol-II 3.2.2.1.18Antivirus Solution for Servers	6-233	The solution should have the option of the endpoint vulnerability shielding in the network.	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
92	Vol-II 3.2.3.1.7Firewall	6-252	The Firewall should be able to manage MFA Tokens to be used for user authentication.	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
93	Vol-II 3.2.3.1.9Firewall	6-252	NGFW should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending a alert and logging the incident	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
94	Vol-II 3.2.3.1.10Firewall	6-253	Firewall should have capability of intelligent routing and failover of traffic on ISP links based on Application Visibility and link Performance SLAs.	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
95	Vol-II 3.2.3.1.12Firewall	6-253	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
96	Vol-II 3.2.3.1.13Firewall	6-254	The proposed system shall allow administrator to prevent sensitive data from leaving the network based on File Type and Extensions. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.
97	Vol-II 3.2.3.1.14Firewall	6-254	IPS solution should have capability to protect against Denial of Service (DOS)/DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.	Recommended to delete	Feature is required vendor can provide with inbuilt or 3rd party solution to meet the functionality.

S/N	Volume/Section No	PageNo	Reference Clause	Clarification Required	NEA Response
98	Vol-II 3.2.3.1.15Firewall	6-254	The proposed firewall shall support 10 logical firewalls	Recommended to delete	As per bid document
99	Vol-II DMS.13 Record Management System	6-203	The system should be certified to Record Management standard like DoD 5015.02 or equivalent standard.	DoD 5015.02 is a standard released by the US Department of Defense in 1997 and revised in 2002. It is relatively old and not suitable for current operating habits. If this standard is followed, it will affect the use of DMS. We propose to remove the requirement of this standard.	As per bid document
100	Vol-I- Section 4: Bidding Forms	4-44	Manufacture's Authorization	Will NEA allow the MAF to be provided by OEM authorized Distribution or reseller for the territory as most of the OEM will work with local partner?	Bidder can submit MAF provided by OEM authorised distributor or reseller for territory in required format along with an authorisation document provided by OEM to authorised distributor or reseller.
101	Vol II /Section 6: Schedule of Requirements	6-204	Additional	From the topology diagram, whether we also need to provide routers, load balancing, and core switches	Bidders need not have to provide routers, load balancers and core switches, as these are not considered in the BoQ

The amendments/clarifications/Addendum issued in this document shall be treated as a part of Bidding Document from here and after and shall be read with the original Bidding Document.

For further details, please contact:
Project Director,
Institutional Strengthening Project (NEA)
Phone: +977-1-4153201/ 4153310 , email: ispnea@gmail.com