SI. No.	RFP Document Reference(s)		Existing Clause	Revised Clause
	RFP Clause No.	**RFP Page No.**		
1	4.5. Performance Bank Guarantee (PBG)	22	Performance Bank Guarantee (PBG) 1. The selected bidder will submit a Performance Bank Guarantee (PBG), after issuance of Purchase order or Work order issued by OCAC as per OGFR rules.	4.5. Performance Bank Guarantee (PBG) 1. The selected bidder will submit a Performance Bank Guarantee (PBG), after issuance of Purchase order or Work order issued by OCAC as per OGFR rules (Performance security should be for an amount of five per cent of the value of the contract.).
2	6.6.7. Item – 7: 2 KVA Online UPS	48	Specification- Warranty for battery 2 Years	**2 KVA Online UPS:** Warranty for battery: 5 Year

RFP for Supply, Installation and Commissioning of Local Area Network and minor electrical work at 110 Health Institutes under OeHMIS Project.
RFP Ref No.: OCAC-HEALTH-INFRA-0001-2024-24058
Corrigendum

Revised Specification

6.6.4. Item – 4: Unified Threat Management (UTM)

Make: (Bidder to Specify)

Model: (Bidder to Specify)

SL No.	Specifications	Compliances (Yes/No)
1	Firewall: Appliance based firewall with build in OS	
2	Should have CLI, GUI and console option	
3	Offered Product should have EAL/ICSA certification and OEM shall be in category in last two published MQ reports of Gartner for UTM Firewall.	

SL No.	Specifications	Compliances (Yes/No)
4	Number of NIC slots, should have minimum 8x 10/100/1000 Mbps Ethernet interfaces, Min 2x SFP/SFP+ interface for fiber connectivity	
5	The Antivirus/Antimalware should have a guaranteed throughput of more than 1.4 Gbps .	
6	Firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet	
7	Number of sessions : should support at least 900k concurrent sessions and 250k DPI connections	
8	Should have a State-full throughput of at least 3.5 Gbps for Firewall	
9	The Intrusion Prevention should have a guaranteed throughput of 2 Gbps or higher	
10	Licensing: should be as per device license and not user/IP based license.	
11	Integrated purpose built in Firewall and VPN: This feature should be easy to configure and use. Should have a support inbuilt for IPSEC VPNs, should support DES, 3 DES and AES (128,192, 256)	
12	Integrated SSL VPN with license for 15 users should be provided from day one.	
13	Firewall should have built in IPS, Antivirus and web filtering license and should get automatically updates from the internet.	
14	Should also have support for Antibot, GeoIP Protection and Data leakage prevention with application control as well	
15	Should have integrated application control. Should be able to define security policy and enforcement for thousands of applications, regardless of the port or the protocol used for communication.	
16	Management: should support management of the box through HTTPS as well as SSH along with console access.	
17	Security Policy: should be easy to configure and manage the firewall policies.	
18	NAT: should support dynamic NAT as well as one-to-one NAT.	
19	Performance: Robust High Level Threat Protection Performance for firewall and VPN and should minimum of 1.5 Gbps firewall Threat Protection throughput and 1.5 Gbps IPSec VPN Throughput	
20	High Availability: The firewall should be able to support high availability (active - active or active - Passive/hot standby)	
21	Multi WAN/ISP support: should support automatic ISP failover as well as ISP load sharing for outbound traffic. Should have separate interfaces for terminating dual ISP Ethernet connectivity.	
22	Traffic Management: option to configure traffic shaping on a per policy basis for specific application/specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy.	
23	The appliance should support VLAN tagging (IEEE 802.1q) and should support VLANs on all interfaces and minimum of 128 VLAN should be Supported	
24	Should have option to block file based on their extension and should have no file size limit on the gateway anti-virus scanning	

SL No.	Specifications	Compliances (Yes/No)
25	The firewall must support cloud and appliance based Sandbox technology and OEM must have their own on-prem and on cloud Advanced Threat Protection solutions	
26	The Firewall should support RIPv1 , RIPv2 OSPF & BGP .	
27	Logging & Reporting : should support secure and generate reports based on the firewall logs	
28	The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc.	
29	Should support min 20K DPI signatures, 60 millions Cloud AV signatures and 3500+ Application Signatures from day one.	
30	Should have configurable options to enable logging at a firewall policy level , log denied traffic details etc.	
31	OEM should have TAC and R&D center in INDIA. Proposed Solution should support 24x7 telephone, email and web-based technical support.	
32	Manufacturer's warranty should be mentioned minimum 05 (Five) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade.	

Revised Tender Schedule:

Last Date of submission of bid: 22.04.2024 by 02:00 PM

Opening of Prequalification & Technical Bids: 22.04.2024 at 03:30 PM

Technical Presentation & Opening of Commercial Bid: To be intimated Later.

(other contents remain unchanged)

RFP for Supply, Installation and Commissioning of Local Area Network and minor electrical work at 110 Health Institutes under OeHMIS Project.					
RFP Ref No.: OCAC-HEALTH-INFRA-0001-2024-24058					
Pre-Bid Resolution					
Sl. No.	RFP Document Reference(s)		Clause Details as per RFP	Query / Clarification / Suggestion	Response
	RFP Clause No.	RFP Page No.			
1	4.5. Performance Bank Guarantee (PBG)	22	Performance Bank Guarantee (PBG) 1. The selected bidder will submit a Performance Bank Guarantee (PBG), after issuance of Purchase order or Work order issued by OCAC as per OGFR rules.	Please accept the BG with 3% of the order value	Please refer the corrigendum.
2	6.1. Detailed Scope of Work	33	Site survey & feasibility is to be undertaken for identification of the actual places in the premises where hardware, network, WiFi, power and earthing points are required to be installed. This task should be completed within 45 days from the date of LoI/PO.	Requesting change in the timeline of site survey as total 110 location is there as per tender. Request to extend another 2 weeks.	As per RFP.
3	6.3. Bill of Materials [BoM]	38	As per BOQ Network active component Both Router and Firewall is mentioned.	We can use Firewall and can use the same device for routing also so one device can be sufficient and by doing this we can eliminate router from BOQ.	As per RFP. (Please refer revised hardware specification)
4	6.6.2. Item – 2: Specifications of Central Core (L3) Switch	42	Performance Requirements-The switch should have minimum 8,000 MAC Address Table size	Request to please change this as "The switch should have minimum 16,000 MAC Address Table size".This is Central switch and capacity should be bit higher than Edge switch.	As per RFP.

5	6.6.2. Item – 2: Specifications of Central Core (L3) Switch	43	Layer-3 Routing and Services Features from day-1- The switch should support IPv4 and IPv6 Static Routing	Request to to please consider "The switch should support IPv4 and IPv6 Static Routing,RIP v1/v2,OSPF".This is L3 so there should be minimum Layer 3 feature available from day-1.	As per RFP.
6	6.6.4. Item – 4: Unified Threat Management (UTM)	45	Specifications- Should also have support for Antibot, GeoIP Protection and Data leakage prevention with application control as well	Request to Remove this point	Please refer the corrigendum.
7	6.6.4. Item – 4: Unified Threat Management (UTM)	45	Specifications- Offered Product should have EAL/ICSA certification and OEM shall be in category in last two published MQ reports of Gartner for UTM Firewall.	Enclosed govt circular with Anexure1	Please refer the corrigendum.
8	6.6.4. Item – 4: Unified Threat Management (UTM)	46	Specifications- The firewall must support cloud or appliance-based Sandbox technology and OEM must have own Advanced Threat Protection solutions.	Sandboxing is generally not utilized in the current scenario due to the prevalence of HTTPS traffic, where data is encrypted, hence request to be removed.	Please refer the corrigendum.
9	6.6.5. Item – 5: Specifications of Wi-Fi Access Point	47	Operational- AP must be offered with required controller software/hardware. AP must support operation in stand-alone or with-controller.	Request to please change this as "AP must support operation in stand-alone or as a controller".	As per RFP.
10	6.6.5. Item – 5: Specifications of Wi-Fi Access Point	47	Antenna- Omni-directional antennas (attached/integrated), Minimum 4 dBi in 2.4GHz and minimum 5 dBi in 5GHz	Requested to change 3.3dBi gain on both antennas instead of 4dbi. The same has been suggested by few of the reputed OEM.	As per RFP.

11	6.6.5. Item – 5: Specifications of Wi-Fi Access Point	47	Request for an addition	Access point should support Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices. This is very relevant for any WLAN environment where client device type is various types which can impact wireless performance.	As per RFP.
12	6.6.5. Item – 5: Specifications of Wi-Fi Access Point	47	Request for an addition	The AP should support Supports priority handling and policy enforcement for unified communication apps, including Skype for Business with encrypted videoconferencing, voice, chat and desktop sharing.	As per RFP.
13	6.6.5. Item – 5: Specifications of Wi-Fi Access Point	47	Request for an addition	Should supports TWT, BSS Wifi 6 features from day-1.	As per RFP.
14	6.6.7. Item – 7: 2 KVA Online UPS	48	Specification- Warranty for battery 2 Years	In the Bill of material clauses of page, no-39, there is mentioned that all the items must have 5year onsite warranty support. Kindly clarify the required warranty for 2KVA Online UPS	Please refer the corrigendum.