Dated :- 17th August'2020

Amendment No - 1

Tender No. HITES /PHOEC-01/20-21

The following amendments are incorporated based on Pre-Bid Meeting held on 12th Aug'2020 (On –Line)

1> Pg.9 , Clause (C) – Is amended as

03 Works of Rs. 1.35 crs. each or Two Works of 02 Crs each or Single Work of Rs. 04 Crs each of such equipments like Server, Storage, LAN Infra , Security Products , Communication Systems , Audio Systems etc. in State / Central Govt. & Large Corporates / Institutions during last 03 years. Copy of work Orders to be submitted.

The revised TECHNICAL Specifications of the Level 2 Switch , Firewall & Access points is as follows :-

Sl.5> Level 2 Switch

S. No.	General Specifications
1.1	**General Features :**
	Proposed switch should be enterprise grade switch with x86 based CPU architecture & should have min of 48 nos. 10/100/1000 Ethernet Ports in addition to 4 10Gig uplink ports.
	Switch should be 1U and rack mountable in standard 19" rack & Switch should support internal hot-swappable Redundant Power supply from day 1.
	Switch should have redundant hot swappable fans & Switch should have minimum 2GB RAM and 2 GB Flash.
	Switch should haven modular stacking, on uplink ports. Should support for minimum 480 Gbps of stacking though put with 8 switch in single stack.
1.2	**Performance :**
	Switch shall have minimum 336 Gbps of switching fabric and 250 Mpps of forwarding rate.
	Switch shall have minimum 32K MAC Addresses and 1000 active VLAN & support minimum 15K IPv4 routes or more and 5K IPv6 routes or more., Switch shall have 8K or more multicast routes & support atleast 64K flow entries, with 128 or more STP Instances. Switch should have 8MB or more packet buffer.
1.3	**Functionality :**
	Should support* advance Layer 3 protocol like BGPv4, BGPv6 , MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP, Switch shall have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.
	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard. Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-256 on hardware.
	During system boots, the system's software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified, it should have cryptographically signed, Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment. Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B o r CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements-. OEM should be listed in Gartner Leader Quadrant for Wired and Wireless LAN .

6 > FIREWALL	
1	The Firewall should be hardware based, reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems.
2	Appliance should have at multicore CPU arch. With hardnet 64 bit OS , support higher memory & should support Min 16 GB of RAM
3	Should support 1.5 Gbps of NGFW & support atleast 200000 concurrent sessions.
4	Should have Integrated Power Supply & Fans
5	Should have High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection. Should have ATP and Pharming Protection. Should have SPX mail encryption. Surfing quota time policies per user/group; Access time polices per user/group Second independent malware detection engine for dual scanning Fully transparent proxy for anti-malware and web-filtering; HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions Enhanced application control with signatures and Layer 7 patterns for applications and E-mail scanning and Anti-Spam with SMTP, POP3, and IMAP support Should provide risk level of applications on the network; Provides visibility into top risk users, unknown applications, advanced threats and suspicious payloads. Should have WAF with reverse proxy. Reputation service with spam outbreak monitoring based on patented Recurrent-Pattern-Detection technology; Malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages Block spam and malware during the SMTP transaction and Detects phishing URLs within e-mails WAF with Reverse proxy; Form hardening engine; SQL injection protection; Cross-site scripting protection; URL hardening engine with deep-linking and directory traversal prevention Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients,

7> Access Points

Generic Requirements
Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave 2. Access Point must have controller functionality to control minimum 15 access points on same LAN.
Must have a robust design for durability, without visible vents.
Mounting kit should be standard from OEM directly.
Must support 4x4 multiple-input multiple-output (MIMO) with four spatial streams
Must support data rates Upto 600 Mbps on 2.4GHz and 1.7Gbps on 5Ghz
Must support up to 26dbm of transmit power in both 2.4Ghz and 5Ghz radios.
Must have 2 nos. of 10/100/1000 Base-T (least one with PoE/PoE+ powering) port and one 1 Multigig port , SSH/Telnet
Must have minimum 16 SSIDs.
Should support detecting and classifying non Wi-Fi wireless transmissions.
Should support radio resource management for power, channel, coverage hole detection and performance optimization.
Must operate as a sensor for wireless IPS.
Access Points must support a distributed encryption/decryption model.
Must be plenum-rated (UL2043).
Should support 802.11e and WMM.

(For HLL INFRA TECH SERVICES LIMITED
(Authorised Signatory)