THE KANGRA CENTRAL CO-OPERATIVE BANK LTD.
DHARAMSHALA

Sehkar Jyoti Building, Civil Lines, Dharamshala,
Teh. Dharamshala, Distt. Kangra, Himachal Pradesh, 176 215, India.

Phone Nos.: +91 1892 – 224969 / 222677 / 223280 / 222353 / 222326
Email: {chairman, md, gmw, gmn, it}@kccb.in
Website: https://www.kccb.in/

Pre-bid Response

RFP Notice No. KCCB/IT/2022/01(A)

Supply, Installation, Implementation, Configuration, Integration, Testing, Commissioning and Maintenance of Compute / Storage and Ancillary Infrastructure, Networking Devices and SDWAN Services at the Data Centre, Disaster Recovery Site and Branch Locations

December, 2022

Response to Pre Bid Queries (Dated June 09, 2023)

Requesting prospective bidder	S No	Section of the Request for Proposal	RFP Clause	Requested Change	Response
Hewlett Packard Enterprise India Pvt. Ltd.	1.	5.3.2, 1	Proposed HCI solution must be present in at least 2 banking customers in India, and must be running the production workload of banks.	Proposed HCI solution must be present in at least 1 banking customers in India, and must be running the production workload of banks." OR "Proposed HCI solution must be present in at least 1 banking customers in India and 2 Government / PSU / Listed customers for production workload.	Accepted. At least 1 Banking Customer.
	2.	5.3.2, 1	The proposed HCI solution must support Data Compression, De-duplication natively and licenses for this feature should be factored in the bill of material.	The proposed HCI solution must support inline Data Compression and De-duplication natively and licenses for this feature should be factored in the bill of material.	Partially accepted. Natively removed.
	3.	5.3.2, 1	The solution should be able to work on latest x86 server hardware available from all the leading vendors in the industry and should not be restricted to a particular vendor / make / model.	This clause is restrictive and favoring certain OEMs. Request to delete this clause.	Not accepted.
	4.	5.3.2, 1	The proposed solution's Hypervisor(s) must offer "Live VM Migration", "High Availability" and intelligent placement of workloads on nodes best suited to their execution.	The proposed solution must offer "Live VM Migration", "High Availability" and intelligent placement of workloads on nodes best suited to their execution.	Not accepted.
	5.	5.3.2, 1	Proposed solution should support synchronous and asynchronous, local and remote replication to the same x86 based HCI appliance in production and remote site. Bank expects <10 mins RPO.	Proposed solution should support synchronous or asynchronous, local and remote replication to the same x86 based HCI appliance in production and remote site. Bank expects <10 mins RPO. Bidder must provision for the same. WAN	Partially accepted. Synchronous, Asynchronous removed.

			Bidder must provision for the same. WAN bandwidth will be provided by the Bank.	bandwidth will be provided by the Bank.	
	6.	5.3.2, 1	Replication & DR automation licenses to be included. There should not be any restriction in number of VM's that can be enabled for replication.	Replication & DR automation licenses for 25VM to be included. There should not be any restriction in number of VM's that can be enabled for replication.	Partially accepted. 50 VM inserted.
	7.	5.3.2, 1	The solution should provide a stateful distributed or virtual firewall that can provide L4-L7 traffic filtering without traffic going to a Physical Firewall.	Request to delete this clause.	Not accepted.
	8.	5.3.2, 1	The proposed solution must be managed through an HTML5 web based console or via virtual appliance that provides a single pane of glass view for the entire environment including 3rd party SAN and VM inventory.	The proposed solution must be managed through an HTML5 web based console or via virtual appliance that provides a single pane of glass view for the entire environment and VM inventory.	Partially accepted. Third Party SAN removed.
	9.	5.3.2, 1	Cluster capacity	We understand capacity asked in the cluster to be provided on SSD disk. Kindly confirm.	Confirmed.
	10.	5.3.2, 1	The Node Configuration at each Site (DC-1 / DC-2):	Please confirm if there is any restriction on number of nodes in particular cluster. We can create cluster with minimum 2 nodes.	Confirmed.
	11.	SD WAN Solution VPN Security:	VPN Security: • The system should allow creation of an encryption policy. • The system should allow an encryption policy to be attached per virtual private network • The system should allow centralized generation of the encryption policy is required	Change Request: VPN Security: • The system should allow creation of an encryption policy/Key. • The system should allow an encryption policy/Key to be attached per virtual private network • The system should allow centralized generation of the encryption policy/Key is required.	Accepted. Document amended accordingly.

	12.	SD WAN Solution Operations and Maintenance Services:	On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device or to activate the device.	Request to remove this clause for wider participation.	Partially accepted. Device replaced with device/port.
	13.	SD WAN Management Controller	The controller must be able to be configured in HA mode to avoid single point of failure	The Orchestrator can be deployed in Active/Backup mode and requires manual effort to make the back up as an active Orchestrator.	Not accepted.
	14.	3. SD-WAN Router for DC / DR	Proposed SDWAN appliance must be rack mountable with minimum of Universal 2 x 1GbE LAN/WAN 1 x USB, 1 x Console, 16 GB RAM, 4 SFP+ Ports, 128 GB SSD	Proposed SDWAN appliance must be rack mountable with minimum of Universal 6 x 1/10GbE SFP+ Ports, 2 x USB, 1 x Console, 16 GB RAM,128 GB SSD	Not accepted.
	15.	3. SD-WAN Router for DC / DR & 4. SD-WAN Router for Branches	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel.	Should support the IPsec VPN deployment modes: hub-and-spoke, full mesh, will be deployed in Router Mode.	Partially accepted. Gateway-to-gateway and redundant tunnel deleted.
	16.	4. SD-WAN Router for Branches	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports, HDMI port.	4. SD-WAN Router for Branches Change Request: Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, 64 GB SSD and 1 USB ports.	Partially accepted. HDMI port removed.
	17.	4. SD-WAN Router for Branches	Proposed device should have single inbuilt SIM SLOT	Request to remove this clause for wider participation	Not accepted.
	18.	SD-WAN - WAN Optimization	New Addition	The SD-WAN Solution should able to mitigate the effects of high WAN latency using TCP acceleration technologies for critical applications	Not accepted.
	19.	SD-WAN - WAN Optimization	New Addition	The SD-WAN Solution should be able to make applications faster and reduce WAN bandwidth utilization using techologies like deduplication (local caching of data), compression and	Not Accepted

				Packet coalescing	
	20.	SD-WAN - WAN Optimizatio n	New Addition	The SD-WAN Solution should be able to mitigate packet loss using FEC and reorder packets arriving out of order	Not accepted.
	21.	Layer2 Features	Switch should support minimum 256,000 no. of MAC addresses.	Switch should support minimum 90K no. of MAC addresses.	Accepted. 256,000 replaced with 64K.
	22.	Layer2 Features	The Switch should Multihoming ESI-LAG.	The Switch should Multihoming ESI-LAG or VSX.	Partially accepted. ESI-LAG or equivalent.
	23.	Layer3 Features	Switch should support RSVP, LDP, 6PE and L3 VPN.	Request to remove this clause.	Accepted. Document amended accordingly.
	24.	Security	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined.	Switch should support for Role Based access control (RBAC) for restricting host level authorization network access as per policy defined.	Accepted. Document amended accordingly.
	25.	New Addition	OS - Securiy	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	Not accepted.
	26.	New Addition	Operating System Capabilities	The switch OS should support programmability through REST APIs and Python scripting or equivalent	Not accepted.
	27.	New Addition	Operating System Capabilities	All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1	Not accepted.
	28.	New Addition		All Switches, Transceivers & SD-WAN shall be from the same OEM. The OEM shall be present in Leaders quadrant in Gartner's Magic Quadrant for Wired and Wireless LAN Access Infrastructure	Not accepted.
	29.	Hardware and Interface Requireme	Switch should have 48 x 10G SFP fiber ports and should have 6 x 40G/100G QSFP28	Switch should have 48 x 10/25G SFP+/SPF28 fiber ports and should have 6 x 40G/100G QSFP28 ports.	Accepted. Document amended accordingly.

		nt	ports.		
	30.	New Addition	Firewall Features inside the switch - To Inspect East - West Servers/Node/VMs Traffic	Switch should support statefull firewall natively into the switch from day 1 for east west traffic or through external hardware appliances meeting the performance specs. Firewall performance required min 750G.	Not accepted.
	31.	New Addition	OS - Security	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	Not accepted.
	32.	New Addition	Operating System Capabilities	The switch should have modular operating system with micro-services or equivalent architecture providing superior fault tolerance and high availability	Not accepted.
	33.	New Addition	Operating System Capabilities	The switch OS should support programmability through REST APIs and Python scripting or equivalent	Not accepted.
	34.	New Addition		All Switches, Transceivers & SD-WAN shall be from the same OEM. The OEM shall be present in Leaders quadrant in Gartner's Magic Quadrant for Wired and Wireless LAN Access Infrastructure	Not accepted.
	35.	Performanc e	Switching fabric of each switch should be minimum 128 Gbps or more. Packet forwarding throughput should be 95 Mpps for packet size of 64 Bytes.	Switching fabric of each switch should be minimum 88 Gbps or more. Packet forwarding throughput should be 65 Mpps for packet size of 64 Bytes.	Accepted. Document amended accordingly.
	36.	Features	The switch should have IPv6 RA Guard and IPv6 Neighbor Discovery Inspection	The switch should have IPv6 RA Guard and IPv6 Neighbor Discovery Inspection or ND snooping.	Partially accepted. Neighbor Discovery Inspection or equivalent.
	37.	Certificatio	The switch should be UL-UL60950-1, FCC Part	The switch should be UL-UL60950-1, FCC, VCCI Class	Partially accepted.

		ns	15, VCCI Class A, EN 55022 / EN 55032, EN 55024 / CISPR32, CAN/CSA 22.2 No.60950-1, Reduction of Hazardous	A, EN 55022 /EN 55024:2010, EN 55024, EN 300386 /EN 61000-3-2:2014 & EN 61000-3-3:2013, CAN/CSA 22.2 No.60950-1, Reduction of Hazardous Substances (ROHS) certified.	Any of the equivalent certifications are also acceptable.
	38.		Switch should be IPv6 (IPv6 Logo ready/ USGv6) certified.	Switch should be IPv6 (IPv6 Logo ready/ USGv6) certified or IPv6 ready.	Accepted. Document amended accordingly.
	39.	Quality of service	It should support Flow-based QoS for traffic prioritization.	It should support Flow-based QoS/DiffServ, COS and Classifier Policies for traffic categorization and prioritization."	Partially accepted. Functionality may be achieved by equivalents means also.
	40.	Quality of service	It should support Eight hardware-based queues per port with Weighted Round Robin (WRR)/ Shaped Round Robin (SRR).	It should support Eight hardware-based queues per port with Weighted Round Robin (WRR)/ Shaped Round Robin (SRR)/DWRR."	Partially accepted. "Or equivalent" added.
	41.	Quality of service	It should support Flow-based bandwidth management, ingress policing; egress rate shaping per port.	It should support Flow-based or Classifier based management, ingress policing/rate-limit; egress rate shaping per port.	Partially accepted. "Or equivalent" added.
	42.	Quality of service	It should have Static routes and support RIP, OSPFv3 in future.	It should have Static routes and support RIPv1/v2, OSPFv3 in future.	Not accepted.
	43.	Standards	RoHSv6 Compliant.	RoHSv6 or RoHS (EN 50581:2012) and WEEE regulations compliant.	Accepted. Document amended accordingly.
	44.	New Addition	OS- Security	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensures the boot process started from a trusted combination of switches."	Not accepted.
	45.	New Addition		All Switches, Transceivers & SD-WAN shall be from the same OEM. The OEM shall be present in Leaders quadrant in Gartner's Magic Quadrant for Wired and Wireless LAN Access Infrastructure	Not accepted.
Cisco Commerce	1.	39	Switch should support RSVP, LDP, 6PE and L3	Request to delete the clause.	Accepted.

India Pvt. Ltd.			VPN.		Document amended accordingly.
	2.	42	HA configuration that uses dedicated 10G HA/ control interface apart from the mentioned traffic interfaces.	HA configuration that uses dedicated/unused 10G HA/ control interface apart from the mentioned traffic interfaces.	Not accepted.
	3.	42	Should support upto 4.5 Million Concurrent sessions and at least 250,000 sessions per second.	Should support upto 4 Million Concurrent sessions and at least 170,000 sessions per second.	Accepted. Document amended accordingly.
	4.	42	Should provide 35 Gbps Firewall Throughput and 20Gbps IMIX throughput.	Should provide 22 Gbps Firewall Throughput and 17 Gbps IMIX throughput.	Not accepted.
	5.	42	Support for: Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman, MD-5, SHA-1, SHA-128, SHA-256.	Support for: Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman,SHA-1, SHA-128, SHA-256.	Partially accepted. MD5 removed.
	6.	43	Internal Redundant Power supply and redundant fans tray	Firewall should have integrated redundant hot-swappable power supply and hot-swappable fan tray / modules	Not accepted.
	7.	31	The SD WAN should have the ability to bind multiple links	The SD WAN should have the ability to load balance between multiple links	Not accepted.
	8.	32	The SD WAN should be able to build connections dynamically between two SDWAN devices leveraging multiple links and apply logic for best path selection, traffic switching, QOS and dynamic link bonding.	The SD WAN should be able to build connections dynamically between two SDWAN devices leveraging multiple links and apply logic for best path selection, traffic switching and QOS.	Not accepted.
	9.	35	On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device or to activate the device.	Request to delete the clause.	Partially accepted. Device replaced with device / port.
	10.	36	The SDWAN appliance		Not accepted.

			must be able to change the role of any ports using system configurations and without re-imaging the software		
	11.	37	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode		Not accepted.
	12.	37	Should include IPsec Configuration Wizard for termination with popular third-party devices		Not accepted.
	13.	37	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports, HDMI port.	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports.	Accepted. Document amended accordingly.
	14.	37	The SDWAN appliance must be able to change the role of the RJ45 ports using system configurations and without re-imaging the software		Not accepted.
	15.	37	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel.		Not accepted.
	16.	37	Should include IPsec Configuration Wizard for termination with popular third-party devices		Not accepted.
	17.	27	The solution should be able to work on latest x86 server hardware available from all the leading vendors in the	The solution should be able to work on latest x86 server hardware available from any leading vendor in the industry and should not be	Not accepted.

			industry and should not be restricted to a particular vendor/make/model	restricted to a particular vendor or make/model.	
	18.	27	The proposed HCI software & hardware should be factory integrated by the OEM as an appliance or license proposed should have flexibility to decouple the HCI software from hardware, in order to run HCI software on any certified hardware.	As per RFP the HCI should either be: Appliance: which has to be factory integrated and tested thoroughly under stringent conditions for end to end compatibility hence the name Appliance. Or when field integrated then the HCI s/w should be capable of running on any certified h/w	Not accepted.
	19.	28	Replication & DR automation licenses to be included. There should not be any restriction in number of VM's that can be enabled for replication	Replication & DR automation licenses to be included. The licensing should be done for approx. 250 VMs based on the asked sizing. An appliance by definition is tested and certified for a set of h/w and s/w as a bundle and is factory integrated and tested for best fail proof performance, compatibility. Theoretically it should work on leading x86 h/w , being from the same family but may not give the same results as an appliance.	Not accepted.
	20.	29	The solution should have catalogue of private as well as public cloud services, and should support self-service provisioning capabilities not limited to only HCI based solution but also for public cloud	The solution should have catalogue of private cloud services, and should support self-service provisioning capabilities for HCI based solution	Not accepted.
	21.	29	The proposed solution should provide application lifecycle management with automated orchestration across multiple hypervisor and cloud	The proposed solution should provide application lifecycle management with automated orchestration across proposed HCI solution	Not accepted.
	22.	30	Cluster2 at DC1	Seems like typo	Not accepted.

			- Total Cores - 190 @ 2.1 GHZ each - RAM - 1152 GB - Usable Storage = 70 TB	error:Cluster2 at DC1 - Cores-2x 32 core @ 2.2 GHZ - RAM - 384 GB - Usable Storage = 23.3 TB	
	23.	30	Cluster2 at DC2: - Total Cores - 190 @ 2.1 GHZ each - RAM - 1152 GB - Usable Storage = 70 TB	Seems like typo error:Cluster2 at DC1 - Cores-2x 32 core @ 2.2 GHZ - RAM - 384 GB - Usable Storage = 23.3 TB	Not accepted.
	24.		The OEM shall be consistently present in Leaders quadrant in Gartner's Magic Quadrant for LAN Access Infrastructure for last five years	To ensure the products should be supplied from consistently leading OEMs	Not accepted.
	25.		Should support IEEE 802.1AE - 128-bit AES MACsec inter network device encryption with MACsec Key Agreement (MKA)	Additional data security without compromising performance of the switch	Not accepted.
	26.		Should have built in platform to Integrate existing security solutions in your environment to unify visibility, enable automation, and strengthen security.		Not accepted.
	27.		Vendor should have built in security intelligence platform to provide access to regularly updated feeds for domains, URLs and IP addresses.		Not accepted.
	28.		The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.		Not accepted.
	29.		Firewall should have a built in storage of minimum 800GB and should be hot		Not accepted.

			swappable		
Infinity Labs Ltd.	1.	5.4.2	The SD WAN should support streaming telemetry/equivalent and RTP protocol for real time monitoring and report purpose.	The SD WAN should support streaming telemetry/equivalent better than traditional SNMP protocol and RTP protocol for real time monitoring and report purpose.	Accepted. Document amended accordingly.
	2.	5.4.2	The solution should comprise of a centralized single plane of Controller/ Manager system which should be placed in DC/ DRC/ Head Office/ Any other site decided by XX-ORGANISATION-XX for automation, device configuration, Policy Orchestration, Software updates etc.	Please confirm if an SDWAN controller is needed in High Availability (HA) mode? And kindly clarify the placement, should one controller be placed in the DC while another in the DRC?	Accepted. Document amended accordingly.
	3.	5.4.2	On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device or to activate the device.	On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device and activate the same through SMS/UI based OTP.	Not accepted.
	4.	5.4.2	The Controller/ Management console should support Zero Touch Provisioning (ZTP) deployment at sites.	The Controller/ Management console should support Zero Touch Provisioning (ZTP) deployment at sites. The plug & play installation/ one touch provisioning through Mobile APP.	Not accepted.
	5.	5.4.2	The solution will allow administrator to forward alerts from the system using email.	The solution will allow administrator to forward alerts from the system using email & SMS.	Not accepted.
	6.	5.4.2	The solution should provide capability of remote diagnostics like Ping, trace route, testing VPN connectivity, Speed test, etc. through a centralized GUI without the requirement of login into CLI of individual branches.	The solution should provide capability of remote diagnostics like Ping, trace route, testing VPN connectivity, Speed test, packet capture, MTR etc. through a centralized GUI without the requirement of login into CLI of individual branches.	Not accepted.
	7.	5.4.2	Proposed SDWAN appliance must be rack mountable with	Proposed SDWAN appliance must be rack mountable with minimum of Universal 6 x	Accepted. Document

			minimum of Universal x 1GbE LAN/WAN 1 x USB, 1 x Console, 16 GB RAM, 4 SFP+ Ports, 128 GB SSD.	1GbE LAN/WAN 2 x USB, 1 x Console, 16 GB RAM, 4 SFP+ Ports, 128 GB SSD.	amended accordingly.
	8.	5.4.2	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports, HDMI port.	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, 64 GB SSD and 2 USB ports, HDMI port. The 2 USB ports can facilitate Branches to work purely on LTE without any wired connectivity dependency.	Not accepted.
	9.	5.4.2	The appliance should have minimum 100 mbps of Aggregated SD-WAN throughput.	The appliance should have minimum 200 Mbps of Aggregated SD-Wan throughput as 100 mbps broadband is quite common and cost effective	Not accepted.
	10.	4.4.9	In addition to the terms and clauses enumerated in this RFP document, all the relevant provisions of General Financial Rules 2017 and any addendum / corrigendum and all the relevant guidelines of CVC and Government of India as well as Government of Himachal Pradesh viz. Make-in-India, Land Border Clause, Incentives to MSMEs / Start-ups and capping on liquidated damages etc. shall be deemed to be part of this RFP document and shall be assumed to have implicitly admitted to by the prospective Bidders.	Make In India - मेक इन इंडिया As per the declaration issued on 31st Aug'21 by the Department of Telecommunications (DOT), Ministry of Telecommunication, Government of India, bearing reference No. 18-10/2017-IP, it has been emphasized that SDWAN Technology and Services within the country have significant local capacity and experience robust local competition. Consequently, it is strongly advised to exclusively consider SDWAN solutions from Make In India Original Equipment Manufacturers (MII OEMs).Our understanding is that SDWAN component & Solution should be from Class- 01 Make In India only, Please Clarify.	Clarified.
	11.		New Point	Configurational changes made at the individual CPE devices locally through the management / console port	Not accepted.

				of the device should be replicated to the controller in case where controller is down / unreachable to make some critical changes in one or few sites.	
Millenimum Automation Pvt. Ltd.	1.	TECHNICAL ELIGIBILITY CRITERIA	The Bidder should have established at least three Data Centres during last 07 years out of which at least one should be functional in a Bank or Govt. establishment in India	The Bidder/OEM should have established at least three Data Centres during last 07 years out of which at least one should be functional in a Bank or Govt. establishment in India	Not accepted.
	2.	TECHNICAL ELIGIBILITY CRITERIA	The Bidder should have established at least three SDWAN setups during last 07 years out of which at least one should be functional in a Bank or Govt. establishment in India	The Bidder/OEM should have established at least three SDWAN setups during last 07 years out of which at least one should be functional in a Bank or Govt. establishment in India	Not accepted.
Juniper Networks Pvt. Ltd.	1.	5.5.2 Specifications	The switch should support 100,000 IPv4 unicast routes and 32,000 IPv6 unicast routes entries in the routing table including 4,000 multicast routes.	The switch should support 100,000 IPv4 unicast routes and 50K IPv6 unicast routes entries in the routing table including 32K multicast routes.	Not accepted.
	2.	5.5.2 Specifications	Switch should support minimum 3 Tbps of switching capacity.	Switch should support minimum 6.4 Tbps of switching capacity.	Not accepted.
	3.	5.5.2 Specifications Top of Rack Switches	Switch should have 48 x 10G SFP fiber ports and should have 6 x 40G/100G QSFP28 ports.	Switch should have 48 x 1/10G/25G SFP/SFP+/SFP28 fiber ports and should have 6 x 40G/100G QSFP28 ports.	Accepted. Document amended accordingly.
	4.	5.5.2 Specifications Top of Rack Switches	Addition	The switch should support 64,000 IPv4 unicast routes and 32,000 IPv6 unicast routes entries in the routing table including 16,000 multicast routes.	Not accepted.
	5.	5.6.2 SPECIFICATIONS Next Generation Firewalls	Should provide 9Gbps NextGen firewall throughput including Firewall, Application security/ AVC, IPS and URL Filtering.	Should provide 9Gbps NextGen firewall throughput including Firewall, Application security/ AVC & IPS.	Accepted. Document amended accordingly.
	6.	5.4.2 TECHNICAL	The SD WAN should have the ability to bind	The SD WAN should have the ability to load share the	Not accepted.

		SPECIFICATIONS SDWAN Solution	multiple links.	traffic on multiple links.	
	7.	5.4.2 TECHNICAL SPECIFICATIONS SDWAN Solution	The SD WAN should support streaming telemetry / equivalent and RTP protocol for real time monitoring and report purpose.	The SD WAN should support streaming telemetry / equivalent and RTP protocol for real time monitoring and report purpose.	Accepted. Document amended accordingly.
	8.	5.4.2 TECHNICAL SPECIFICATIONS SDWAN Solution	The solution must provide Remote diagnostics tools to validate reachability of both WAN and LAN side, Packet Capture, Packet flow CLI tracer etc.	The solution must provide Remote diagnostics tools to validate reachability of both WAN and LAN side, Packet Capture, Ping and traceroute etc.	Not accepted.
	9.	5.4.2 TECHNICAL SPECIFICATIONS SDWAN Solution	The SD WAN solution should support encryptions for end to end communication. The solution should use standard encryption technology, such as AES256/above to provide secure connectivity over any type of WAN link. Rekeying functionality should be available in the solution for encryptions.	The SD WAN solution should support encryptions for end to end communication. The solution should use standard encryption technology, such as AES256/above to provide secure connectivity over any type of WAN link. Rekeying/Static Keys functionality should be available in the solution for encryptions.	Not accepted.
	10.	5.4.2 TECHNICAL SPECIFICATIONS VPN Security:	The system should implement a secure virtual private network that connects the branch locations, and data centers on one single managed network. The system should allow creation of an encryption policy. The system should allow an encryption policy to be attached per virtual private network The system should allow centralized generation of the	Request to remove this clause as these features are not mandatory features in SDWAN solution as may not be relevant for every OEM IPSec VPNs is not the only solution for security. Security can be achieved via deployed various solutions/encryption mechanism which are FIPS compliant secondly creating IPSec tunnel at every locations may eat 20-30% available bandwidth only for control plane/IKE session traffic.	Not accepted.

			encryption policy is required The system should allow dynamic tunnels to be created without any static overlays between branch and the hub. The system should allow for full mesh connectivity between the Data Center and the branch locations The system should allow for hub-and-spoke connectivity between the data center (hub) and the branch, (spokes). The system should ensure that any change in connectivity (Link 1 to Link 2 connectivity in case of multiple links being terminated on the branch device) does not require any change in virtual private network configuration in the controller or physical/virtual device at location The system should be able to automatically pick the tunnel encapsulation type based on the application and based on the policy specified in the software defined network controller. The system should support the encryption algorithms for Data Security The system should ensure that virtual private network configuration and policy is performed in the controller. The addition of one or more branch devices in to the network should not		

			require any changes in the virtual private network configuration in software defined network controller		
	11.	5.4.2 TECHNICAL SPECIFICATIONS SD-WAN Reporting	The solution must support syslog and email / SMS based alarm to notify the administrators when any device / link fault or network performance degradation happens	The solution must support syslog and email / SMS based alarm to notify the administrators when any device / link fault or network performance degradation happens or solution should support 3rd party integration using REST APIs.	Not accepted.
	12.	5.4.2 TECHNICAL SPECIFICATIONS SD-WAN Reporting	The solution needs to be flexible enough to support customization in case of any unique requirements with the availability of the OEM engineering/support team in India	The solution needs to be flexible enough to support customization in case of any unique requirements with the availability of the OEM engineering/support team in India subject to features available for the proposed solution.	Not accepted.
	13.	SD WAN Management Controller	Solution should have privilege level of users like L-1, L-2 and L-3 to control and to manage deployed SD-WAN devices.	Solution should have privilege level of users like L-1, L-2 and L-3 to control and to manage deployed SD-WAN devices or role based access control.	Not accepted.
	14.	5.4.2 TECHNICAL SPECIFICATIONS SDWAN Solution	SDWAN Solution	SDWAN is a design / Architecture rather than device or protocol. We request to have functional requirements to enable leading OEMs to participate and offer their SDWAN solution.	Not accepted.
Takyon Networks Pvt. Ltd.	1.	4.4.9	All the relevant guidelines of CVC and Government of India as well as Government of Himachal Pradesh viz. Make-in-India, Land Border Clause, Incentives to MSMEs / Start-ups and capping on liquidated damages etc. shall be deemed to be part of this RFP document	Start-ups are exempted from prior work experience criteria, Kindly confirm bidders who are registered as start up with Govt. of India are exempted from prior work experience.	Confirmed.
	2.	4.13, RATES	The rates quoted shall remain firm throughout	Quoted rates depends on dollar value also, We request	Not accepted.

			the period of contract and this contract will remain valid till the date of completion of the job by the Bidder(s) and shall not be subject to any upward modification whatsoever.	you to kindly consider dollar fluctuation and any increase in dollar value beyond 5% shall increase the quoted rates in proportion of same.	
	3.	b. Preventative maintenance	The Vendor agrees to physically inspect the systems for potential problems at least once a quarter	The Vendor agrees to physically inspect the systems at Data Centre for potential problems at least once a quarter	Partially accepted. Once in a semester.
	4.	BOQ_100645	S No 1.04, Quantity 1	This basically denotes the SDWAN heading, and all SDWAN components are included from S No 1.05 to 1.07. Kindly confirm shall bidder put zero value against this serial number.	Confirmed.
	5.	BOQ_100645	S No 1.05, SD WAN Management Controller - Quantity 1	On RFP page no 30 under scope of work clause no 5.4.1(bi) , RFP has asked for deploying and setting up the SDWAN at both DC & DR, therefore We would request you to kindly change the quantity to 2	Accepted. Document amended accordingly.
ZEN Exim Pvt. Ltd.	1.	3. Stackable PoE Switches	Certifications The switch should be UL-UL60950-1, FCC Part 15, VCCI Class A, EN 55022, EN 55024, EN 300386, CAN/CSA 22.2 No.60950-1, Reduction of Hazardous Substances (ROHS) or equivalent certified. Switch should be IPv6 (IPv6 Logo ready/ USGv6) certified. Switch Should be Common Criteria EAL3/CC/NDcPP certified or equivalent.	The switch should be UL-UL60950-1 / FCC Part 15 / VCCI Class A / EN 55022 / EN 55024 / EN 300386 / CAN/CSA 22.2 No.60950-1 / Reduction of Hazardous Substances (ROHS) or equivalent certified. Switch should be IPv6 (IPv6 Logo ready/ USGv6) certified / IPv6 ready from day one. Switch Should be Common Criteria EAL3/CC/NDcPP certified/VAPT Certified or equivalent.	Partially accepted. All equivalent Indian certifications are acceptable.
Calculus Business	1.	9	The SD WAN should support one way latency and traffic loss monitoring	The SD WAN should support one two way latency and traffic loss monitoring.	Not accepted.
	2.	6	The SD WAN must provide following	The SD WAN must provide following reports of	Not accepted.

			reports of Individual link quality/ Virtual link quality on daily, weekly, monthly, yearly etc.: - Packet loss in the links - Hop Counts - Latency of links	Individual link quality/ Virtual link quality on daily, weekly, monthly, yearly etc.: - Packet loss in the links - Hop Counts - Latency of links, MoS score based traffic steering, FEC, Packet cloning, TCP optimization, AppQoS[shaping / rate limiting.	
	3.	6	The system architecture should allow the use the most preferred link based upon Link characteristics (Latency, Hop Count, Packet Loss, Jitter) for critical applications as defined in policy	The system architecture should allow the use the most preferred link based upon Link characteristics (Latency, Hop Count, Packet Loss, Jitter, MoS score based traffic steering, FEC, Packet cloning, TCP optimization, AppQoS[shaping/ratelimiting]) for critical applications as defined in policy	Not accepted.
	4.	1	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, 64 GB SSD and 2 USB ports, HDMI port.	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, 64 GB SSD and 2 USB ports, HDMI port.	Accepted. Document amended accordingly.
	5.	10	Should support the IPsec VPN deployment modes: hub- and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode	Should support the IPsec VPN deployment modes: hub- and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode, tunnel mode.	Not accepted.
	6.	2	Network Statistics including continuous performance monitoring of loss, latency, and packet ordering for all network paths and link utilization.	Network Statistics including continuous performance monitoring of loss, latency, packet ordering for all network paths and link utilization.	Not accepted.
	7.	5.6.2	Next Generation Firewalls-Should provide Stateful failover.	Next Generation Firewalls-Should provide Stateful/Stateless failover.	Not accepted.
	8.	5.6.2	Next Generation Firewalls	NGFW should provide Vulnerability Profiles - by	Not accepted.

				CVE ID/signature set /CVSS Score/Packet direction/Class,	
	9.	5.6.2	Next Generation Firewalls	NGFW should provide Multiple Vulnerability DB Reference	Not accepted.
	10.	5.6.2	Next Generation Firewalls	NGFW should provide Packet capture - pre & post window, Signature based & Protocol Anomaly based and L7 anomaly detection	Not accepted.
	11.	5	SD-WAN Router for Branches : SDWAN appliance must be capable of terminating broadband, ILL, MPLS, 3G/4G, PPPoE connectivity	SDWAN appliance must be capable of terminating broadband, ILL, MPLS, 3G/4G, PPPoE connectivity and WiFi LAN connectivity to branch users.	Not accepted.
	12.	6	The SD WAN device should have the capability to forward traffic via specific WAN paths depending on predefined application policies and performance needs.	The SD WAN device should have the capability to forward traffic via specific WAN paths depending on predefined application policies and performance needs. AppQoS – Traffic shaping, AppQoS – Rate limiting and Selective application encryption (ie: encryption based on app or traffic type).App based intelligent path selection – user-defined criteria, least cost, high bandwidth paths.	Not accepted.
Velocis Systems Pvt. Ltd.	1.	39	Switch should support RSVP, LDP, 6PE and L3 VPN.	Request to delete the clause.	Accepted. Document amended accordingly.
	2.	42	HA configuration that uses dedicated 10G HA/ control interface apart from the mentioned traffic interfaces.	HA configuration that uses dedicated/unused 10G HA/ control interface apart from the mentioned traffic interfaces.	Not accepted.
	3.	42	Should support upto 4.5 Million Concurrent sessions and at least 250,000 sessions per second.	Should support upto 4 Million Concurrent sessions and at least 170,000 sessions per second.	Accepted. Document amended accordingly.
	4.	42	Should provide 35 Gbps Firewall Throughput and 20Gbps IMIX throughput.	Should provide 22 Gbps Firewall Throughput and 17 Gbps IMIX throughput.	Not accepted.

	5.	42	Support for: Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman, MD-5, SHA-1, SHA-128, SHA-256.	Support for: Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman,SHA-1, SHA-128, SHA-256.	Partially accepted. MD5 removed.
	6.	43	Internal Redundant Power supply and redundant fans tray	Firewall should have integrated redundant hot-swappable power supply and hot-swappable fan tray / modules	Not accepted.
	7.	31	The SD WAN should have the ability to bind multiple links	The SD WAN should have the ability to load balance between multiple links	Not accepted.
	8.	32	The SD WAN should be able to build connections dynamically between two SDWAN devices leveraging multiple links and apply logic for best path selection, traffic switching, QOS and dynamic link bonding.	The SD WAN should be able to build connections dynamically between two SDWAN devices leveraging multiple links and apply logic for best path selection, traffic switching and QOS.	Partially accepted. Device replaced with device / port.
	9.	35	On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device or to activate the device.	Request to delete the clause.	Not accepted.
	10.	36	The SDWAN appliance must be able to change the role of any ports using system configurations and without re-imaging the software		Not accepted.
	11.	37	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode		Not accepted.
	12.	37	Should include IPsec Configuration Wizard for termination with		Not accepted.

			popular third-party devices		
	13.	37	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports, HDMI port.	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports.	Accepted. Document amended accordingly.
	14.	37	The SDWAN appliance must be able to change the role of the RJ45 ports using system configurations and without re-imaging the software		Not accepted.
	15.	37	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel.		Not accepted.
	16.	37	Should include IPsec Configuration Wizard for termination with popular third-party devices		Not accepted.
	17.	27	The proposed HCI software & hardware should be factory integrated by the OEM as an appliance or license proposed should have flexibility to decouple the HCI software from hardware, in order to run HCI software on any certified hardware.	As per RFP the HCI should either be: 1) Appliance: which has to be factory integrated and tested thoroughly under stringent conditions for end to end compatibity hence the name Appliance. Or (b)when field integrated then the HCI s/w should be capable of running on any certified h/w	Not accepted.
	18.	27	The solution should be able to work on latest x86 server hardware available from all the leading vendors in the industry and should not be restricted to a particular vendor/make/model	The solution should be able to work on latest x86 server hardware available from any leading vendor in the industry and should not be restricted to a particular vendor or make/model.	Not accepted.

	19.	28	Replication & DR automation licenses to be included. There should not be any restriction in number of VM's that can be enabled for replication	Replication & DR automation licenses to be included. The licensing should be done for approx. 250 VMs based on the asked sizing.	Partially Accepted. 50 VM inserted.
	20.	29	The solution should have catalogue of private as well as public cloud services, and should support self-service provisioning capabilities not limited to only HCI based solution but also for public cloud	The solution should have catalogue of private cloud services, and should support self-service provisioning capabilities for HCI based solution	Not accepted.
	21.	29	The proposed solution should provide application lifecycle management with automated orchestration across multiple hypervisor and cloud	The proposed solution should provide application lifecycle management with automated orchestration across proposed HCI solution	Not accepted.
	22.	30	Cluster2 at DC1 - Total Cores - 190 @ 2.1 GHZ each - RAM - 1152 GB - Usable Storage = 70 TB	Seems like typo error:Cluster2 at DC1 - Cores-2x 32 core @ 2.2 GHZ - RAM - 384 GB - Usable Storage = 23.3 TB	Not accepted.
	23.	30	Cluster2 at DC2: - Total Cores - 190 @ 2.1 GHZ each - RAM - 1152 GB - Usable Storage = 70 TB	Seems like typo error:Cluster2 at DC1 - Cores-2x 32 core @ 2.2 GHZ - RAM - 384 GB - Usable Storage = 23.3 TB	Not accepted.
Airtel	1.	18	WARRANTY AND SUPPORT	We request Kangra bank to consider the warranty from date of delivery not from date of installation.	Not accepted.
	2.	20	TRAININGS	We request Kangra Bank to share the scope of training in details.	Clarified.
	3.		c. Uptime:	We request Kangra Bank to consider the uptime 99% for remote locations.	Not accepted.
	4.		General	All kind of permission/access at site from feasibility check to link delivery will be arranged by customer.	Clarified.

				In building internal cable routing in false celling and under POP wall will be in customer scope of work	
	5.		General	RACK Space, Proper UPS power supply and earthing arrangement for the bidder devices will be arranged and maintained by customer.	Clarified.
	6.		General	All the equipments delivered by bidder at customer site for the Services should be kept under safe custody by the customer. In case any device found lost or damaged due to customer attribute than customer has to bear the cost for lost/damaged as well as new device.	Clarified.
	7.		General	NO SLA penalty will be applicable on bidder incase the location is down due to 1) Power issue at customer end. 2) Improper earthing at site. 3) Equipment damaged due to water seepage or stolen from the location. 4) Access not available at site for the bidder engineer to check the issue. 5) LC not available at site. 6) Any condition which is beyond the control of bidder.	Clarified.
	8.	35	5.4.2 TECHNICAL SPECIFICATIONS-Operations and Maintenance Services: Point 7	Request to delete : In Case of BB & Dynamic WAN IP the device will raise false alarm and this will deactivate the device. So Request to delete this clause	Not accepted.
	9.	33	5.4.2 TECHNICAL SPECIFICATIONS-Centralized Management, Monitoring and Configuration	Request to replace with-NMS capabilities can be built by a separate NMS tool for network visibility of all the devices	Not accepted.
	10.	18	4.13	Quoted rates depends on lot of factors and making it firm for period of five years is not a feasible option. We	Not accepted.

				request you to kindly delete this clause.	
	11.	30	5.4.1	Kindly confirm rack for SDWAN controller and Routers at DC/DR and Branches will be provided by the bank	Clarified.
	12.	59	Preventative Maintenance	Since bank has asked for comprehensive maintenance, and physical inspection of 250 locations in every quarter is not feasible option, we request you to kindly delete this clause.	Partially Accepted. Once in a semester.
	13.		Operation and Maintenance:	We request Kangra bank to share the scope details and quantity of resources with field resources. Also please share the shift timing of resources.	Clarified.
VM-Ware	1.	5.3.2	Proposed solution should support synchronous and asynchronous, local and remote replication to the same x86 based HCI appliance in production and remote site. Bank expects <10 mins RPO. Bidder must provision for the same. WAN bandwidth will be provided by the Bank.	Proposed solution should provide synchronous or asynchronous, local and remote replication to same x86 based HCI in production and remote site. Bank expects <10 mins RPO. Bidder must provision for the same. WAN bandwidth will be provided by the bank.	Accepted. Document amended accordingly.
Cyfuture Pvt. Ltd.	1.	39	Switch should support RSVP, LDP, 6PE and L3 VPN.	Request to delete the clause.	Accepted. Document amended accordingly.
	2.	42	HA configuration that uses dedicated 10G HA/ control interface apart from the mentioned traffic interfaces.	HA configuration that uses dedicated/unused 10G HA/ control interface apart from the mentioned traffic interfaces.	Not accepted.
	3.	42	Should support upto 4.5 Million Concurrent sessions and at least 250,000 sessions per second.	Should support upto 4 Million Concurrent sessions and at least 170,000 sessions per second.	Accepted. Document amended accordingly.
	4.	42	Should provide 35 Gbps Firewall Throughput and 20Gbps IMIX	Should provide 22 Gbps Firewall Throughput and 17 Gbps IMIX throughput.	Not accepted.

			throughput.		
	5.	42	Support for: Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman, MD-5, SHA-1, SHA-128, SHA-256.	Support for: Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman,SHA-1, SHA-128, SHA-256.	Partially accepted. MD5 removed.
	6.	43	Internal Redundant Power supply and redundant fans tray	Firewall should have integrated redundant hot-swappable power supply and hot-swappable fan tray / modules	Not accepted.
	7.	31	The SD WAN should have the ability to bind multiple links	The SD WAN should have the ability to load balance between multiple links	Not accepted.
	8.	32	The SD WAN should be able to build connections dynamically between two SDWAN devices leveraging multiple links and apply logic for best path selection, traffic switching, QOS and dynamic link bonding.	The SD WAN should be able to build connections dynamically between two SDWAN devices leveraging multiple links and apply logic for best path selection, traffic switching and QOS.	Not accepted.
	9.	35	On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device or to activate the device.	Request to delete the clause.	Partially accepted. Device replaced with device / port.
	10.	36	The SDWAN appliance must be able to change the role of any ports using system configurations and without re-imaging the software	Required further clarity on the roles required and use case for this requirement. (We can change the port into transport mode/service mode)	Not accepted.
	11.	37	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode	Requires revalidation on 'VPN termination in transparent mode' aspect. (we support hub-and-spoke, full mesh, partial mesh, per VPN topology, regional Mesh etc.)	Not accepted.
	12.	37	Should include IPsec Configuration Wizard	Better to understand the use case for termination with	Not accepted.

			for termination with popular third-party devices	popular third- party devices (We can do with Zscaler, umbrella Sig, Netskope)	
	13.	37	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports, HDMI port.	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports.	Accepted. Document amended accordingly.
	14.	37	The SDWAN appliance must be able to change the role of the RJ45 ports using system configurations and without re-imaging the software	Required further clarity on the roles required and use case for this requirement. (We can change the port into transport mode/service mode)	Not accepted.
	15.	37	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel.	Requires clarification. (we support hub-and-spoke, full mesh, partial mesh, per VPN topology, regional Mesh etc.)	Not accepted.
	16.	37	Should include IPsec Configuration Wizard for termination with popular third-party devices	Better to understand the use case for termination with popular third- party devices. Please let us know the third party devices (We can do with Zscaler, umbrella Sig, Netskope these are cloud proxies.)	Not accepted.
	17.	27	The solution should be able to work on latest x86 server hardware available from all the leading vendors in the industry and should not be restricted to a particular vendor/make/model	The solution should be able to work on latest x86 server hardware available from any leading vendor in the industry and should not be restricted to a particular vendor or make/model.	Not accepted.
	18.	28	Replication & DR automation licenses to be included. There should not be any restriction in number of VM's that can be enabled for replication	Replication & DR automation licenses to be included. The licensing should be done for approx. 250 VMs based on the asked sizing.	Partially accepted. 50 VMs included.
	19.	29	The solution should have catalogue of	The solution should have catalogue of private cloud	Not accepted.

			private as well as public cloud services, and should support self-service provisioning capabilities not limited to only HCI based solution but also for public cloud	services, and should support self-service provisioning capabilities for HCI based solution	
	20.	29	The proposed solution should provide application lifecycle management with automated orchestration across multiple hypervisor and cloud	The proposed solution should provide application lifecycle management with automated orchestration across proposed HCI solution	Not accepted.
	21.	30	Cluster2 at DC1 - Total Cores - 190 @ 2.1 GHZ each - RAM - 1152 GB - Usable Storage = 70 TB	Seems like typo error:Cluster2 at DC1 - Cores-2x 32 core @ 2.2 GHZ - RAM - 384 GB - Usable Storage = 23.3 TB	Not accepted.
	22.	30	Cluster2 at DC2: - Total Cores - 190 @ 2.1 GHZ each - RAM - 1152 GB - Usable Storage = 70 TB	Seems like typo error:Cluster2 at DC1 - Cores-2x 32 core @ 2.2 GHZ - RAM - 384 GB - Usable Storage = 23.3 TB	Not accepted.
	23.	Access Switch	Additional Suggestions	The OEM shall be consistently present in Leaders quadrant in Gartner's Magic Quadrant for LAN Access Infrastructure for last five years	Not accepted.
	24.	Access Switch	Additional Suggestions	Should support IEEE 802.1AE - 128-bit AES MACsec inter network device encryption with MACsec Key Agreement (MKA)	Not accepted.
	25.	Next Generation Firewalls	Additional Suggestions	Should have built in platform to Integrate existing security solutions in your environment to unify visibility, enable automation, and strengthen security.	Not accepted.
	26.	Next Generation Firewalls	Additional Suggestions	Vendor should have built in security intelligence platform to provide access to regularly updated feeds for domains, URLs and IP addresses.	Not accepted.

	27.	Next Generation Firewalls	Additional Suggestions	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.	Not accepted.
	28.	Next Generation Firewalls	Additional Suggestions	Firewall should have a built in storage of minimum 800GB and should be hot swappable	Not accepted.
	29.	28	Proposed solution should support synchronous and asynchronous, local and remote replication to the same x86 based HCI appliance in production and remote site. Bank expects <10 mins RPO. Bidder must provision for the same. WAN bandwidth will be provided by the Bank.	Proposed solution should provide synchronous or asynchronous, local and remote replication to same x86 based HCI in production and remote site . Bank expects <10 mins RPO. Bidder must provision for the same. WAN bandwidth will be provided by the bank	Partially accepted. Synchronous and asynchronous removed.
TNS Networking Solutions Pvt. Ltd.	1.	6.5	Detail about tender fee & Earnest money deposit	Kindly Clarify the mode of payment will be online or offline if online kindly share the payment link	Clarified.
	2.	4.2	The Bidder should have established at least three Data Centres during last 05 years out of which at least one should be functional in a Bank or Govt. establishment in India.	The Bidder/OEM should have established at least three Data Centres during last 05 years out of which at least one should be functional in a Bank or Govt. establishment in India.	Not accepted.
	3.	5.6.2	Change in specs of Next Generation Firewalls (I.e. Management - Accessible through variety of methods including Telnet, Console Port, SSH.)	Device shall have remote manageability features like https/webui & SSH.	Not accepted.
	4.	5.6.2	Change in specs of Next Generation Firewalls (I.e. Certification- The Firewall should be EAL 3 / NDPP / NDcPP or equivalent certified under Common Criteria.)	The Firewall should be EAL 3 / NDPP / NDcPP / ICSA or equivalent certified under Common Criteria.	Partially accepted. Equivalent Indian certifications are also acceptable.

Pace Info Solutions Pvt. Ltd.	1.	5.3.2, 1, Hyper Converged Infrastructure	Proposed HCI solution must be present in at least 2 banking customers in India, and must be running the production workload of banks.	Proposed HCI solution must be present in at least 1 banking customers in India, and must be running the production workload of banks." OR "Proposed HCI solution must be present in at least 1 banking customers in India and 2 Government / PSU / Listed customers for production workload.	Accepted. At least 1 Banking Customer.
	2.	5.3.2, 1, Hyper Converged Infrastructure	The proposed HCI solution must support Data Compression, De-duplication natively and licenses for this feature should be factored in the bill of material.	The proposed HCI solution must support inline Data Compression and De-duplication natively and licenses for this feature should be factored in the bill of material.	Partially Accepted. Natively removed.
	3.	5.3.2, 1, Hyper Converged Infrastructure	The solution should be able to work on latest x86 server hardware available from all the leading vendors in the industry and should not be restricted to a particular vendor / make / model.	This clause is restrictive and favouring certain OEMs. Request to delete this clause.	Not Accepted.
	4.	5.3.2, 1, Hyper Converged Infrastructure	The proposed solution's Hypervisor(s) must offer "Live VM Migration", "High Availability" and intelligent placement of workloads on nodes best suited to their execution.	The proposed solution must offer "Live VM Migration", "High Availability" and intelligent placement of workloads on nodes best suited to their execution.	Not Accepted.
	5.	5.3.2, 1, Hyper Converged Infrastructure	Proposed solution should support synchronous and asynchronous, local and remote replication to the same x86 based HCI appliance in production and remote site. Bank expects <10 mins RPO. Bidder must provision for the same. WAN bandwidth will be provided by the Bank.	Proposed solution should support synchronous or asynchronous, local and remote replication to the same x86 based HCI appliance in production and remote site. Bank expects <10 mins RPO. Bidder must provision for the same. WAN bandwidth will be provided by the Bank.	Partially Accepted. Synchronous, Asynchronous removed.
	6.	5.3.2, 1, Hyper Converged	Replication & DR automation licenses to be included. There	Replication & DR automation licenses for 25VM to be included. There should not	Partially Accepted. 50 VM inserted.

		Infrastructure	should not be any restriction in number of VM's that can be enabled for replication.	be any restriction in number of VM's that can be enabled for replication.	
	7.	5.3.2, 1, Hyper Converged Infrastructure	The solution should provide a stateful distributed or virtual firewall that can provide L4-L7 traffic filtering without traffic going to a Physical Firewall.	Request to delete this clause.	Not Accepted.
	8.	5.3.2, 1, Hyper Converged Infrastructure	The proposed solution must be managed through an HTML5 web based console or via virtual appliance that provides a single pane of glass view for the entire environment including 3rd party SAN and VM inventory.	The proposed solution must be managed through an HTML5 web based console or via virtual appliance that provides a single pane of glass view for the entire environment and VM inventory.	Partially Accepted. Third Party SAN removed.
	9.	5.3.2, 1, Hyper Converged Infrastructure	Cluster capacity	We understand capacity asked in the cluster to be provided on SSD disk. Kindly confirm.	Confirmed.
	10	5.3.2, 1, Hyper Converged Infrastructure	The Node Configuration at each Site (DC-1 / DC-2):	Please confirm if there is any restriction on number of nodes in particular cluster. We can create cluster with minimum 2 nodes.	Confirmed.
	11.	SD WAN Solution VPN Security:	VPN Security: • The system should allow creation of an encryption policy. • The system should allow an encryption policy to be attached per virtual private network • The system should allow centralized generation of the encryption policy is required	Change Request: VPN Security: • The system should allow creation of an encryption policy/Key. • The system should allow an encryption policy/Key to be attached per virtual private network • The system should allow centralized generation of the encryption policy/Key is required.	Accepted. Document amended accordingly.
	12.	SD WAN Solution Operations and Maintenance Services:	On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device or to activate the device.	Request to remove this clause for wider participation.	Partially accepted. Device replaced with device/port.

	13.	SD WAN Management Controller	The controller must be able to be configured in HA mode to avoid single point of failure	The Orchestrator can be deployed in Active/Backup mode and requires manual effort to make the back up as an active Orchestrator.	Not Accepted.
	14.	3. SD-WAN Router for DC / DR	Proposed SDWAN appliance must be rack mountable with minimum of Universal 2 x 1GbE LAN/WAN 1 x USB, 1 x Console, 16 GB RAM, 4 SFP+ Ports, 128 GB SSD	Proposed SDWAN appliance must be rack mountable with minimum of Universal 6 x 1/10GbE SFP+ Ports, 2 x USB, 1 x Console, 16 GB RAM,128 GB SSD	Not Accepted.
	15.	3. SD-WAN Router for DC / DR & 4. SD-WAN Router for Branches	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel.	Should support the IPsec VPN deployment modes: hub-and-spoke, full mesh, will be deployed in Router Mode.	Partially accepted. Gateway-to-gateway and redundant tunnel deleted.
	16.	4. SD-WAN Router for Branches	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports, HDMI port.	4. SD-WAN Router for Branches Change Request: Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, 64 GB SSD and 1 USB ports.	Partially accepted. HDMI port removed.
	17.	4. SD-WAN Router for Branches	Proposed device should have single inbuilt SIM SLOT	Request to remove this clause for wider participation	Not accepted.
	18.	SD-WAN - WAN Optimization	New Addition	The SD-WAN Solution should able to mitigate the effects of high WAN latency using TCP acceleration technologies for critical applications	Not accepted.
	19.	SD-WAN - WAN Optimization	New Addition	The SD-WAN Solution should be able to make applications faster and reduce WAN bandwidth utilization using technologies like deduplication (local caching of data), compression and Packet coalescing	Not Accepted
	20.	SD-WAN - WAN Optimization	New Addition	The SD-WAN Solution should be able to mitigate packet loss using FEC and reorder packets arriving out of order	Not accepted.

	21.	Layer2 Features	Switch should support minimum 256,000 no. of MAC addresses.	Switch should support minimum 90K no. of MAC addresses.	Accepted. 256,000 replaced with 64K.
	22.	Layer2 Features	The Switch should Multihoming ESI-LAG.	The Switch should Multihoming ESI-LAG or VSX.	Partially Accepted. ESI-LAG or equivalent.
	23.	Layer3 Features	Switch should support RSVP, LDP, 6PE and L3 VPN.	Request to remove this clause.	Accepted. Document amended accordingly.
	24.	Security	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined.	Switch should support for Role Based access control (RBAC) for restricting host level authorization network access as per policy defined.	Accepted. Document amended accordingly.
	25.	New Addition	OS - Securiy	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	Not accepted.
	26.	New Addition	Operating System Capabilities	The switch OS should support programmability through REST APIs and Python scripting or equivalent	Not accepted.
	27.	New Addition	Operating System Capabilities	All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1	Not accepted.
	28.	New Addition		All Switches, Transceivers & SD-WAN shall be from the same OEM. The OEM shall be present in Leaders quadrant in Gartner's Magic Quadrant for Wired and Wireless LAN Access Infrastructure	Not accepted.
	29.	Hardware and Interface Requirement	Switch should have 48 x 10G SFP fiber ports and should have 6 x 40G/100G QSFP28 ports.	Switch should have 48 x 10/25G SFP+/SPF28 fiber ports and should have 6 x 40G/100G QSFP28 ports.	Accepted. Document amended accordingly.
	30.	New Addition	Firewall Features inside the switch - To Inspect East - West Servers/Node/VMs	Switch should support statefull firewall natively into the switch from day 1 for east west traffic or through	Not accepted.

			Traffic	external hardware appliances meeting the performance specs. Firewall performance required min 750G.	
	31.	New Addition	OS - Security	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches."	Not accepted.
	32.	New Addition	Operating System Capabilities	The switch should have modular operating system with micro-services or equivalent architecture providing superior fault tolerance and high availability	Not accepted.
	33.	New Addition	Operating System Capabilities	The switch OS should support programmability through REST APIs and Python scripting or equivalent	Not accepted.
	34.	New Addition		All Switches, Transceivers & SD-WAN shall be from the same OEM. The OEM shall be present in Leaders quadrant in Gartner's Magic Quadrant for Wired and Wireless LAN Access Infrastructure	Not accepted.
	35.	Performanc e	Switching fabric of each switch should be minimum 128 Gbps or more. Packet forwarding throughput should be 95 Mpps for packet size of 64 Bytes.	Switching fabric of each switch should be minimum 88 Gbps or more. Packet forwarding throughput should be 65 Mpps for packet size of 64 Bytes.	Accepted. Document amended accordingly.
	36.	Features	The switch should have IPv6 RA Guard and IPv6 Neighbor Discovery Inspection	The switch should have IPv6 RA Guard and IPv6 Neighbor Discovery Inspection or ND snooping.	Partially accepted. Neighbor Discovery Inspection or equivalent.
	37.	Certificatio ns	The switch should be UL-UL60950-1, FCC Part 15, VCCI Class A, EN 55022 / EN 55032, EN 55024 / CISPR32, CAN/CSA 22.2 No.60950-1, Reduction	The switch should be UL-UL60950-1, FCC, VCCI Class A, EN 55022 /EN 55024:2010, EN 55024, EN 300386 /EN 61000-3-2:2014 & EN 61000-3-3:2013, CAN/CSA 22.2 No.60950-1,	Partially Accepted. Any of the equivalent certifications are also acceptable.

			of Hazardous	Reduction of Hazardous Substances (ROHS) certified.	
	38.		Switch should be IPv6 (IPv6 Logo ready/ USGv6) certified.	Switch should be IPv6 (IPv6 Logo ready/ USGv6) certified or IPv6 ready.	Accepted. Document amended accordingly.
	39.	Quality of service	It should support Flow-based QoS for traffic prioritization.	It should support Flow-based QoS/DiffServ, COS and Classifier Policies for traffic categorization and prioritization."	Partially accepted. Functionality may be achieved by equivalents means also.
	40.	Quality of service	It should support Eight hardware-based queues per port with Weighted Round Robin (WRR)/ Shaped Round Robin (SRR).	It should support Eight hardware-based queues per port with Weighted Round Robin (WRR)/ Shaped Round Robin (SRR)/DWRR."	Partially Accepted. "Or equivalent" added.
	41.	Quality of service	It should support Flow-based bandwidth management, ingress policing; egress rate shaping per port.	It should support Flow-based or Classifier based management, ingress policing/rate-limit; egress rate shaping per port.	Partially Accepted. "Or equivalent" added.
	42.	Quality of service	It should have Static routes and support RIP, OSPFv3 in future.	It should have Static routes and support RIPv1/v2, OSPFv3 in future.	Not accepted.
	43.	Standards	RoHSv6 Compliant.	RoHSv6 or RoHS (EN 50581:2012) and WEEE regulations compliant.	Accepted. Document amended accordingly.
	44.	New Addition	OS- Security	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensures the boot process started from a trusted combination of switches."	Not accepted.
	45.	New Addition		All Switches, Transceivers & SD-WAN shall be from the same OEM. The OEM shall be present in Leaders quadrant in Gartner's Magic Quadrant for Wired and Wireless LAN Access Infrastructure	Not accepted.
RV Solutions Pvt. Ltd , Noida	1.	5.2.1(a)	Supply, Installation	Kindly clarify whether complete Infra of alternate power i.e DG Sets,ISP services till POP is available till Data Center.Is the cable laid between ISP POP till	Clarified.

				Data Center	
	2.		General	Kindly share the Lay out diagram and size of DC and DR so that exact estimate of passives are done	Clarified.
	3.		General	SLA of the service Provider to determine the uptime of SDWAN	Clarified.
	4.	5.3.2, 1, Hyper Converged Infrastructure	Proposed HCI solution must be present in at least 2 banking customers in India, and must be running the production workload of banks.	Proposed HCI solution must be present in at least 1 banking customers in India, and must be running the production workload of banks. OR Proposed HCI solution must be present in at least 1 banking customers in India and 2 Governement / PSU / Listed customers for production workload.	Accepted. At least 1 Banking Customer.
	5.	5.3.2, 1, Hyper Converged Infrastructure	The proposed HCI solution must support Data Compression, De-duplication natively and licenses for this feature should be factored in the bill of material.	The proposed HCI solution must support inline Data Compression and De-duplication natively and licenses for this feature should be factored in the bill of material."	Partially Accepted. Natively removed.
	6.	5.3.2, 1, Hyper Converged Infrastructure	The solution should be able to work on latest x86 server hardware available from all the leading vendors in the industry and should not be restricted to a particular vendor/make/model.	This clause is restrictive and favoring certain OEMs. Request to delete this clause.	Not Accepted.
	7.	5.3.2, 1, Hyper Converged Infrastructure	The proposed solution's Hypervisor(s) must offer "Live VM Migration", "High Availability" and intelligent placement of workloads on nodes best suited to their execution.	Not all OEM solutions are dependent on Hypervisor to deliver asked functionality. Request you to modify clause as "The proposed solution must offer "Live VM Migration", "High Availability" and intelligent placement of workloads on nodes best suited to their execution."	Not Accepted.
	8.	5.3.2, 1, Hyper Converged	Proposed solution should support synchronous and	Current clause is restrictive for many OEMs and is not inline with RPO of <10 mins.	Partially Accepted. Synchronous, Asynchronous

		Infrastructure	asynchronous, local and remote replication to the same x86 based HCI appliance in production and remote site. Bank expects <10 mins RPO. Bidder must provision for the same. WAN bandwidth will be provided by the Bank	Proposed solution should support synchronous or asynchronous, local and remote replication to the same x86 based HCI appliance in production and remote site. Bank expects <10 mins RPO. Bidder must provision for the same. WAN bandwidth will be provided by the Bank	removed.
	9.	5.3.2, 1, Hyper Converged Infrastructure	Replication & DR automation licenses to be included. There should not be any restriction in number of VM's that can be enabled for replication.	Request to modify clause as "Replication & DR automation licenses for 25VM to be included. There should not be any restriction in number of VM's that can be enabled for replication.	Partially Accepted. 50 VM inserted.
	10.	5.3.2, 1, Hyper Converged Infrastructure	The solution should provide a stateful distributed or virtual firewall that can provide L4-L7 traffic filtering without traffic going to a Physical Firewall.	This clause is restrictive and favoring certain OEMs. Request to delete this clause.	Not Accepted.
	11.	5.3.2, 1, Hyper Converged Infrastructure	The proposed solution must be managed through an HTML5 web based console or via virtual appliance that provides a single pane of glass view for the entire environment including 3rd party SAN and VM inventory.	There is no SAN array asked in RFP. This clause is restrictive and favoring certain OEMs. Request to modify this clause as "The proposed solution must be managed through an HTML5 web based console or via virtual appliance that provides a single pane of glass view for the entire environment and VM inventory."	Partially Accepted. Third Party SAN removed.
	12.	5.3.2, 1, Hyper Converged Infrastructure	Cluster capacity	We understand capacity asked in the cluster to be provided on SSD disk. Kindly confirm.	Confirmed.
	13.	5.3.2, 1, Hyper Converged Infrastructure	The Node Configuration at each Site (DC-1 / DC-2):	Please confirm if there is any restriction on number of nodes in particular cluster. We can create cluster with minimum 2 nodes.	Confirmed.
	14.	SD WAN Solution VPN	VPN Security: • The system should allow creation of an	Change Request: VPN Security: • The system should allow	Accepted. Document amended

		Security:	encryption policy. • The system should allow an encryption policy to be attached per virtual private network • The system should allow centralized generation of the encryption policy is required	creation of an encryption policy/Key. • The system should allow an encryption policy/Key to be attached per virtual private network • The system should allow centralized generation of the encryption policy/Key is required	accordingly.
	15.	SD WAN Solution Operations and Maintenance Services:	On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device or to activate the device.	Request to remove this clause for wider participation	Partially accepted. Device replaced with device/port.
	16.	SD WAN Management Controller	The controller must be able to be configured in HA mode to avoid single point of failure	Change Request: The Orchestrator can be deployed in Active/Backup mode and requires manual effort to make the back up as an active Orchestrator.	Not Accepted.
	17.	3. SD-WAN Router for DC / DR	Proposed SDWAN appliance must be rack mountable with minimum of Universal 2 x 1GbE LAN/WAN 1 x USB, 1 x Console, 16 GB RAM, 4 SFP+ Ports, 128 GB SSD	3. SD-WAN Router for DC / DR Chante Request: Proposed SDWAN appliance must be rack mountable with minimum of Universal 6 x 1/10GbE SFP+ Ports, 2 x USB, 1 x Console, 16 GB RAM,128 GB SSD	Not Accepted.
	18.	3. SD-WAN Router for DC / DR & 4. SD-WAN Router for Branches	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel.	3. SD-WAN Router for DC / DR & 4. SD-WAN Router for Branches Change Request: Should support the IPsec VPN deployment modes: hub[1]and-spoke, full mesh, will be deployed in Router Mode	Partially accepted. Gateway-to-gateway and redundant tunnel deleted.
	19.	4. SD-WAN Router for Branches	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports, HDMI port.	4. SD-WAN Router for Branches Change Request: Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, 64 GB SSD and 1 USB ports.	Partially accepted. HDMI port removed.
	20.	4. SD-WAN	Proposed device should	Request to remove this	Not accepted.

		Router for Branches	have single inbuilt SIM SLOT	clause for wider participation	
	21.	SD-WAN Features (Path Conditionin g + QoS)	New Addition		Not accepted.
	22.	SD-WAN - WAN Optimizatio n	New Addition	The SD-WAN Solution should able to mitigate the effects of high WAN latency using TCP acceleartion technologies for critical applications	Not accepted.
	23.	SD-WAN - WAN Optimizatio n	New Addition	The SD-WAN Solution should be able to make applications faster and reduce WAN bandwidth utilization using technologies like deduplication (local caching of data), compression and Packet coalescing	Not Accepted
	24.	SD-WAN - WAN Optimizatio n	New Addition	The SD-WAN Solution should be able to mitigate packet loss using FEC and reorder packets arriving out of order	Not accepted.
	25.	Layer2 Features	Switch should support minimum 256,000 no. of MAC addresses.	Since technology and architecture differs from OEM to OEM. Switch support 98K mac addresses table, which is sufficient for Spine/core switch. Because in solution there is also requiremnet of TOR switches and can also be used to restrict the layer-2 boundries/broadcast. Request you to kindly modify the clause as "Switch should support minimum 90K no. of MAC addresses" so that leading OEM can participate.	Accepted. 256,000 replaced with 64K.
	26.	Layer2 Features	The Switch should Multihoming ESI-LAG.	The Switch should Multihoming ESI-LAG or VSX.	Partially Accepted. ESI-LAG or equivalent.
	27.	Layer3 Features	Switch should support RSVP, LDP, 6PE and L3 VPN.	HPE aruba Switch support all data center environment protocol like RIPng, OSPF, BGP, MP-BGP etc. All the MPLS level requirement and end to end bandwidth reservation is generally	Accepted. Document amended accordingly.

				required at service provider level. Request to remove this clause. solution doesn't require any such protocol.	
	28.	Security	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined.	Switch should support for Role Based access control (RBAC) for restricting host level authorization network access as per policy defined.	Accepted. Document amended accordingly.
	29.	New Addition	OS - Securiy	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	Not accepted.
	30.	New Addition	Operating System Capabilities	The switch OS should support programmability through REST APIs and Python scripting or equivalent	Not accepted.
	31.	New Addition	Operating System Capabilities	All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1	Not accepted.
	32.	New Addition		All Switches, Transceivers & SD-WAN shall be from the same OEM. The OEM shall be present in Leaders quadrant in Gartner's Magic Quadrant for Wired and Wireless LAN Access Infrastructure	Not accepted.
	33.	Hardware and Interface Requirement	Switch should have 48 x 10G SFP fiber ports and should have 6 x 40G/100G QSFP28 ports.	Switch should have 48 x 10/25G SFP+/SPF28 fiber ports and should have 6 x 40G/100G QSFP28 ports.	Accepted. Document amended accordingly.
	34.	New Addition	Firewall Features inside the switch - To Inspect East - West Servers/Node/VMs Traffic	Switch should support stateful firewall natively into the switch from day 1 for east west traffic or through external hardware appliances meeting the performance specs. Firewall performance required min 750G.	Not accepted.
	35.	New Addition	OS - Security	The Switch should support integrated trusted platform module (TPM) for platform	Not accepted.

				integrity. This ensure the boot process started from a trusted combination of switches.	
	36.	New Addition	Operating System Capabilities	The switch should have modular operating system with micro-services or equivalent architecture providing superior fault tolerance and high availability	Not accepted.
	37.	New Addition	Operating System Capabilities	The switch OS should support programmability through REST APIs and Python scripting or equivalent	Not accepted.
	38.	New Addition		All Switches, Transceivers & SD-WAN shall be from the same OEM. The OEM shall be present in Leaders quadrant in Gartner's Magic Quadrant for Wired and Wireless LAN Access Infrastructure	Not accepted.
	39.	Performanc e	Switching fabric of each switch should be minimum 128 Gbps or more. Packet forwarding throughput should be 95 Mpps for packet size of 64 Bytes.	Switching fabric of each switch should be minimum 88 Gbps or more. Packet forwarding throughput should be 65 Mpps for packet size of 64 Bytes.	Accepted. Document amended accordingly.
	40.	Features	The switch should have IPv6 RA Guard and IPv6 Neighbor Discovery Inspection	The switch should have IPv6 RA Guard and IPv6 Neighbor Discovery Inspection or ND snooping.	Partially accepted. Neighbor Discovery Inspection or equivalent.
	41.	Certificatio ns	The switch should be UL-UL60950-1, FCC Part 15, VCCI Class A, EN 55022 / EN 55032, EN 55024 / CISPR32, CAN/CSA 22.2 No.60950-1, Reduction of Hazardous	The switch should be UL-UL60950-1, FCC, VCCI Class A, EN 55022 /EN 55024:2010, EN 55024, EN 300386 /EN 61000-3-2:2014 & EN 61000-3-3:2013, CAN/CSA 22.2 No.60950-1, Reduction of Hazardous Substances (ROHS) certified.	Partially Accepted. Any of the equivalent certifications are also acceptable.
	42.		Switch should be IPv6 (IPv6 Logo ready/ USGv6) certified.	Switch should be IPv6 (IPv6 Logo ready/ USGv6) certified or IPv6 ready.	Accepted. Document amended accordingly.
	43.	Quality of	It should support Flow-	It should support Flow-based	Partially accepted.

		service	based QoS for traffic prioritization.	QoS/DiffServ, COS and Classifier Policies for traffic categorization and prioritization."	Functionality may be achieved by equivalents means also.
	44.	Quality of service	It should support Eight hardware-based queues per port with Weighted Round Robin (WRR)/ Shaped Round Robin (SRR).	It should support Eight hardware-based queues per port with Weighted Round Robin (WRR)/ Shaped Round Robin (SRR)/DWRR."	Partially Accepted. "Or equivalent" added.
	45.	Quality of service	It should support Flow-based bandwidth management, ingress policing; egress rate shaping per port.	It should support Flow-based or Classifier based management, ingress policing/rate-limit; egress rate shaping per port.	Partially Accepted. "Or equivalent" added.
	46.	Quality of service	It should have Static routes and support RIP, OSPFv3 in future.	It should have Static routes and support RIPv1/v2, OSPFv3 in future.	Not accepted.
	47.	Standards	RoHSv6 Compliant.	RoHSv6 or RoHS (EN 50581:2012) and WEEE regulations compliant.	Accepted. Document amended accordingly.
	48.	New Addition	OS- Security	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensures the boot process started from a trusted combination of switches."	Not accepted.
	49.	New Addition		All Switches, Transceivers & SD-WAN shall be from the same OEM. The OEM shall be present in Leaders quadrant in Gartner's Magic Quadrant for Wired and Wireless LAN Access Infrastructure	Not accepted.
	50.	5.5.2 Specification Layer3 Features	Switch should support RSVP, LDP, 6PE and L3 VPN.	Request to delete the clause.	Accepted. Document amended accordingly.
	51.	5.6.2 Next Generation Firewalls	HA configuration that uses dedicated 10G HA/ control interface apart from the mentioned traffic interfaces.	HA configuration that uses dedicated/unused 10G HA/ control interface apart from the mentioned traffic interfaces.	Not accepted.
	52.	5.6.2 Next Generation Firewalls	Should support upto 4.5 Million Concurrent sessions and at least 250,000 sessions per second.	Should support upto 4 Million Concurrent sessions and at least 170,000 sessions per second.	Accepted. Document amended accordingly.

	53.	Certificatio n	The Firewall should be EAL 3 / NDPP / NDcPP certified under Common Criteria.	Kindly remove the clause and in corporate as "As per public procurement under MEITY, preference must be given to Make In India cyber security products". Against EAL ICSA test certification by labs may be accepted.	Partially accepted. All equivalent Indian certifications are acceptable.
	54.	System Throughput	Should provide 35 Gbps Firewall Throughput and 20Gbps IMIX throughput.	Should provide 22 Gbps Firewall Throughput and 17 Gbps IMIX throughput.	Not accepted.
	55.	Supports	Support for: Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman, MD-5, SHA-1, SHA-128, SHA-256.	Support for: Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman,SHA-1, SHA-128, SHA-256.	Partially accepted. MD5 removed.
	56.	Power Supply	Internal Redundant Power supply and redundant fans tray	Firewall should have integrated redundant hot-swappable power supply and hot-swappable fan tray / modules	Not accepted.
	57.	5.4.2 TECHNICAL SPECIFICATI ONS	The SD WAN should have the ability to bind multiple links	The SD WAN should have the ability to load balance between multiple links	Not accepted.
	58.	5.4.2	The SD WAN should be able to build connections dynamically between two SDWAN devices leveraging multiple links and apply logic for best path selection, traffic switching, QOS and dynamic link bonding.	The SD WAN should be able to build connections dynamically between two SDWAN devices leveraging multiple links and apply logic for best path selection, traffic switching and QOS.	Not accepted.
	59.	Operations and Maintenan ce Services:	On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device or to activate the device.	Request to delete the clause.	Partially accepted. Device replaced with device / port.
	60.	SD WAN Manageme nt Controller	The SDWAN appliance must be able to change the role of any ports using system configurations and		Not accepted.

			without re-imaging the software		
	61.	SD-WAN Router for DC / DR	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode		Not accepted.
	62.	SD-WAN Router for DC / DR	Should include IPsec Configuration Wizard for termination with popular third-party devices		Not accepted.
	63.	SD-WAN Router for Branches	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports, HDMI port.	Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (10/100/1000 RJ-45) Ports, 8GB RAM, and 1 USB ports.	Accepted. Document amended accordingly.
	64.	SD-WAN Router for Branches	The SDWAN appliance must be able to change the role of the RJ45 ports using system configurations and without re-imaging the software		Not accepted.
	65.	SD-WAN Router for Branches	Should support the IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel.		Not accepted.
	66.	SD-WAN Router for Branches	Should include IPsec Configuration Wizard for termination with popular third-party devices		Not accepted.
	67.	5.3.2 SPECIFICATIONS HCI ARCHITECTURE	The solution should be able to work on latest x86 server hardware available from all the leading vendors in the industry and should not be restricted to a particular	The solution should be able to work on latest x86 server hardware available from any leading vendor in the industry and should not be restricted to a particular vendor or make/model.	Not accepted.

			vendor/make/model		
	68.	5.3.2 REPLICATION	Replication & DR automation licenses to be included. There should not be any restriction in number of VM's that can be enabled for replication	Replication & DR automation licenses to be included. The licensing should be done for approx. 250 VMs based on the asked sizing. An appliance by definition is tested and certified for a set of h/w and s/w as a bundle and is factory integrated and tested for best fail proof performance, compatibility. Theoretically it should work on leading x86 h/w , being from the same family but may not give the same results as an appliance.	Not accepted.
	69.	5.3.2 CLOUD MANAGEMENT PLATFORM	The solution should have catalogue of private as well as public cloud services, and should support self-service provisioning capabilities not limited to only HCI based solution but also for public cloud	The solution should have catalogue of private cloud services, and should support self-service provisioning capabilities for HCI based solution	Not accepted.
	70.	5.3.2 CLOUD MANAGEMENT PLATFORM	The proposed solution should provide application lifecycle management with automated orchestration across multiple hypervisor and cloud	The proposed solution should provide application lifecycle management with automated orchestration across proposed HCI solution	Not accepted.
	71.	5.3.2 The Node Configuration at each Site (DC-1 / DC-2):	Cluster2 at DC1 - Total Cores - 190 @ 2.1 GHZ each - RAM - 1152 GB - Usable Storage = 70 TB	Seems like typo error:Cluster2 at DC1 - Cores-2x 32 core @ 2.2 GHZ - RAM - 384 GB - Usable Storage = 23.3 TB	Not accepted.
	72.	5.3.2 The Node Configuration at each Site (DC-1 / DC-2):	Cluster2 at DC1 - Total Cores - 190 @ 2.1 GHZ each - RAM - 1152 GB - Usable Storage = 70 TB	Seems like typo error:Cluster2 at DC1 - Cores-2x 32 core @ 2.2 GHZ - RAM - 384 GB - Usable Storage = 23.3 TB	Not accepted.
	73.	Access Switch	Additional	The OEM shall be consistently present in Leaders quadrant in Gartner's Magic Quadrant for LAN Access Infrastructure	Not accepted.

				for last five years	
	74.	Access Switch	Additional	Should support IEEE 802.1AE - 128-bit AES MACsec inter network device encryption with MACsec Key Agreement (MKA)	Not accepted.
	75.	Access Switch	Additional	Should have built in platform to Integrate existing security solutions in your environment to unify visibility, enable automation, and strengthen security.	Not accepted.
	76.	Next Generation Firewall	Additional	Vendor should have built in security intelligence platform to provide access to regularly updated feeds for domains, URLs and IP addresses.	Not accepted.
	77.		Additional	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.	Not accepted.
	78.		Additional	Firewall should have a built in storage of minimum 800GB and should be hot swappable	Not accepted.
Future Netwings Solutions Pvt. Ltd.	1.		The Bidders may form consortia of at most 2 separate companies. In case of consortia, all the relevant qualifying criteria must be met simultaneously.	We understand that in case a bidder forms a consortium, the technical eligibility criteria must be met by either the lead bidder or the consortium partner i.e. can the lead bidder use the credentials of the consortium for the Qualifying criteria specified as per clause 4.1, 4.2 & 4.3.	Clarified.
	2.	Terms & Conditions of the Request for Proposal	The Bidder should have established at least three Data Centres or should have established at least three SDWAN setups during last 07 years out of which at least one should be functional in a Bank or Govt. establishment in India.	The lead bidder/Consortium partner should have established at least three Data Centres or should have established at least three SDWAN Setup during last 07 years out of which at least one should be functional in a bank or Govt. establishment in India either directly or indirectly (i.e. by	Accepted. Document amended accordingly.

			Copy of Purchase Orders, or Contracts or Letters of Appreciation should be enclosed as Annexure ET-1/B.	subcontracting).	
	3.	4.2 TECHNICAL ELIGIBILITY CRITERIA: S. No. 1	Earnest Money shall be deposited offline in the form of Bank Guarantee / Cheques / Demand Draft (scanned copy should be uploaded on e-procurement portal https://hptenders.gov.in/) as directed on the portal of the Government of Himachal Pradesh with the bid. The applicable payable amount is ₹ 20,00,000/- (Rupees Twenty Lacs only) for each schedule. In case any prospective bidder intends to quote for both the schedules the applicable payable amount would be ₹ 40,00,000/- (Rupees Forty Lacs only).	It is requested to kindly confirm in case of consortium, MSME exemption against EMD will be valid if any one of the consortium partner comes under MSME category.	Clarified. In case the lead bidder is MSME, the consortium shall get that exemption.
	4.	4.12 EARNEST MONEY DEPOSIT (EMD)	The switch should support 100,000 IPv4 unicast routes and 32,000 IPv6 unicast routes entries in the routing table including 4,000 multicast routes.	The switch should support 100,000 IPv4 unicast routes and 50K IPv6 unicast routes entries in the routing table including 32K multicast routes.	Not accepted.
	5.	5.5.2 Specifications	Switch should support minimum 3 Tbps of switching capacity.	Switch should support minimum 6.4 Tbps of switching capacity.	Not accepted.
	6.	5.5.2 Specifications	Switch should have 48 x 10G SFP fiber ports and should have 6 x 40G/100G QSFP28 ports.	Switch should have 48 x 1/10G/25G SFP/SFP+/SFP28 fiber ports and should have 6 x 40G/100G QSFP28 ports.	Accepted. Document amended accordingly.
	7.	5.5.2 Specifications Top of Rack Switches	Addition	The switch should support 64,000 IPv4 unicast routes and 32,000 IPv6 unicast routes entries in the routing table including 16,000 multicast routes.	Not accepted.
	8.	5.5.2	The earnest money	It is requested to kindly	Clarified.

		Specifications Top of Rack Switches	deposit has been revised to ₹ 20,00,000/- (Rupees Twenty Lakh for each schedule).	confirm in case of consortium, MSME exemption against EMD will be valid if any one of the consortium partner comes under MSME category .	In case the lead bidder is MSME, the consortium shall get that exemption.
Delta Electronics India Private Limited	1.	5.2.2 Technical Specifications Point no 1.	42U Rack, 1000Wx1200Dx2000H, IP-54 Racks to ensure protection against ingress of dust and water.	Width of Rack shall be 800W as per industry standard and IP54 rating shall be removed as it is not applicable being installation in indoor premises.	Not accepted.
	2.	5.2.2 Technical Specifications Point no 1.	Sturdy frame having 9X folding profile welded construction	Please mention multi-fold.	Not accepted.
	3.	5.2.2 Technical Specifications Point no 1.	Unique 3-Point Locking System with Ergo-form handle & unique safety key for front & back door	Unique 3 point locking shall be removed, as already Biometric lock is mentioned in the RFP.	Not accepted.
	4.	5.2.2 Technical Specifications Point no 1.	Increased corrosion resistance using state of art paint technology (Nano ceramic coat, EC dip coat & powder coated painting)	Nano Ceramic & Electro dip coat is OEM specific and shall be removed. Instead we propose GI sheet with Epoxy power coating.	Not accepted.
	5.	5.2.2 Technical Specifications Point no 1.	The cooling system shall be zero U rack based type with horizontal uniform cold air distribution with (N + 1) redundancy.	Instead zero U we propose Rack mount cooling unit	Not accepted.
	6.	5.2.2 Technical Specifications Point no 1.	The cold air distribution shall be lateral, uniform from 1U to 42U in front of the 19” equipment for efficient cooling.	Being Rack mount cooling there will be little non-uniform airflow distribution at top of rack, but there shall not be any issue in performance of IT equipment so requesting to remove this	Not accepted.
	7.	5.2.2 Technical Specifications Point no 1.	All monitored data and alarms can be sent via network by sending e-mail and sms alerts	Instead sms alerts we propose email alerts which is more authentic	Not accepted.
	8.	5.2.2 Technical Specificatio	Airflow sensor	Airflow sensor is OEM specific so requesting to remove	Not accepted.

		ns Point no 1.			
	9.	5.2.2 Technical Specifications Point no 1.	Rack based very early smoke detection system	Rack based Very Early Smoke detection system is OEM specific, and not required for 2 Rack solution.	Not accepted.
	10.	5.2.2 Technical Specifications Point no 1.	The fire suppression system shall be 1U 19 inch rack mount solution for early fire detection & automatic fire extinguishing using eco-friendly NOVEC 1230 clean agent gas.	Instead rack mount fire suppression, we propose external rack side mount fire suppression system to save internal rack U space	Not accepted.
	11.	5.2.2 Technical Specifications Point no 1.	Vertical basic PDU, 32A, Single Phase, C13 Sockets - 16nos, C19 Sockets - 4nos, 32A DP MCB with cover, Power cord of 6sqmm x 3core cable with pin type lugs.	Instead 16 nos. C-13 sockets, we propose 14 nos. C13 and 4 nos. C-19 sockets and additional 6 nos. 5/15 Amp Indian sockets – total 24 sockets	Not accepted.
Targus Technologies (Pvt.) Ltd.	1.	5.5.2 Specifications	The switch should support 100,000 IPv4 unicast routes and 32,000 IPv6 unicast routes entries in the routing table including 4,000 multicast routes.	The switch should support 100,000 IPv4 unicast routes and 50K IPv6 unicast routes entries in the routing table including 32K multicast routes.	Not accepted.
	2.	5.5.2 Specifications	Switch should support minimum 3 Tbps of switching capacity.	Switch should support minimum 6.4 Tbps of switching capacity.	Not accepted.
	3.	5.5.2 Specifications Top of Rack Switches	Switch should have 48 x 10G SFP fiber ports and should have 6 x 40G/100G QSFP28 ports.	Switch should have 48 x 1/10G/25G SFP/SFP+/SFP28 fiber ports and should have 6 x 40G/100G QSFP28 ports.	Accepted. Document amended accordingly.
	4.	5.5.2 Specifications Top of Rack Switches	Addition	The switch should support 64,000 IPv4 unicast routes and 32,000 IPv6 unicast routes entries in the routing table including 16,000 multicast routes.	Not accepted.
	5.	5.6.2 SPECIFICATIONS Next Generation	Should provide 9Gbps NextGen firewall throughput including Firewall, Application security/ AVC, IPS and	Should provide 9Gbps NextGen firewall throughput including Firewall, Application security/ AVC & IPS.	Accepted. Document amended accordingly.

		Firewalls	URL Filtering.		
	6.	5.4.2 TECHNICAL SPECIFICATIONS SDWAN Solution	The SD WAN should have the ability to bind multiple links.	The SD WAN should have the ability to load share the traffic on multiple links.	Not accepted.
	7.	5.4.2 TECHNICAL SPECIFICATIONS SDWAN Solution	The SD WAN should support streaming telemetry / equivalent and RTP protocol for real time monitoring and report purpose.	The SD WAN should support streaming telemetry / equivalent and RTP protocol for real time monitoring and report purpose.	Accepted. Document amended accordingly.
	8.	5.4.2 TECHNICAL SPECIFICATIONS SDWAN Solution	The solution must provide Remote diagnostics tools to validate reachability of both WAN and LAN side, Packet Capture, Packet flow CLI tracer etc.	The solution must provide Remote diagnostics tools to validate reachability of both WAN and LAN side, Packet Capture, Ping and traceroute etc.	Not accepted.
	9.	5.4.2 TECHNICAL SPECIFICATIONS SDWAN Solution	The SD WAN solution should support encryptions for end to end communication. The solution should use standard encryption technology, such as AES256/above to provide secure connectivity over any type of WAN link. Rekeying functionality should be available in the solution for encryptions.	The SD WAN solution should support encryptions for end to end communication. The solution should use standard encryption technology, such as AES256/above to provide secure connectivity over any type of WAN link. Rekeying/Static Keys functionality should be available in the solution for encryptions.	Not accepted.
	10.	5.4.2 TECHNICAL SPECIFICATIONS VPN Security:	The system should implement a secure virtual private network that connects the branch locations, and data centers on one single managed network. The system should allow creation of an encryption policy. The system should allow an encryption policy to be attached per virtual private	Request to remove this clause as these features are not mandatory features in SDWAN solution as may not be relevant for every OEM IPSec VPNs is not the only solution for security. Security can be achieved via deployed various solutions/encryption mechanism which are FIPS compliant secondly creating IPSec tunnel at every locations may eat 20-30% available bandwidth only for control plane/IKE session	Not accepted.

			network. The system should allow centralized generation of the encryption policy is required. The system should allow dynamic tunnels to be created without any static overlays between branch and the hub. The system should allow for full mesh connectivity between the Data Center and the branch locations. The system should allow for hub-and-spoke connectivity between the data center (hub) and the branch, (spokes). The system should ensure that any change in connectivity (Link 1 to Link 2 connectivity in case of multiple links being terminated on the branch device) does not require any change in virtual private network configuration in the controller or physical/virtual device at location. The system should be able to automatically pick the tunnel encapsulation type based on the application and based on the policy specified in the software defined network controller. The system should support the encryption algorithms for Data Security. The system should ensure that virtual private network configuration and	traffic.	

			policy is performed in the controller. The addition of one or more branch devices in to the network should not require any changes in the virtual private network configuration in software defined network controller.		
	11.	5.4.2 TECHNICAL SPECIFICATIONS SD-WAN Reporting	The solution must support syslog and email / SMS based alarm to notify the administrators when any device / link fault or network performance degradation happens	The solution must support syslog and email / SMS based alarm to notify the administrators when any device / link fault or network performance degradation happens or solution should support 3rd party integration using REST APIs.	Not accepted.
	12.	5.4.2 TECHNICAL SPECIFICATIONS SD-WAN Reporting	The solution needs to be flexible enough to support customization in case of any unique requirements with the availability of the OEM engineering/support team in India.	The solution needs to be flexible enough to support customization in case of any unique requirements with the availability of the OEM engineering/support team in India subject to features available for the proposed solution.	Not accepted.
	13.	SD WAN Management Controller	Solution should have privilege level of users like L-1, L-2 and L-3 to control and to manage deployed SD-WAN devices.	Solution should have privilege level of users like L-1, L-2 and L-3 to control and to manage deployed SD-WAN devices or role based access control.	Not accepted.
	14.	5.4.2 TECHNICAL SPECIFICATIONS SDWAN Solution	SDWAN Solution	SDWAN is a design / Architecture rather than device or protocol. We request to have functional requirements to enable leading OEMs to participate and offer their SDWAN solution.	Not accepted.
Suo Motto	1.	The bid is bifurcated in two separate schedules, one each for DC/DR compute and storage and the Bank network plus security appliances respectively. In case a bidder is interested to quote for only one schedule, they must mark ₹ 0/- (Rupees Nil) in all the BOQ line items for the other schedule. The BOQ item number B ie. "Annual charges towards Operation of DC and DR sites for next 05 years after successful testing and sign off" may be used for quoting the cost of competent staff (60 man months) for operation of DC/DR or SDWAN as the case may be. The bidders intending to bid for both the schedules, the cost may be provided for operating the DC/DR as well as SDWAN (120 man months). The Bidders are advised to quote only unit cost in the relevant cell of the BOQ disregarding			

		the quantities mentioned therein. The bids will be evaluated based upon the notional quantities mentioned in the revised Request for Proposal Document and are subject to change. In such cases, the payment shall be as per actual.
	2.	During the prebid, as per requests of multiple prospective bidders, the commercials were agreed to be asked comprehensively for 05 years in place of 03 years. The published BOQ cannot be modified at this stage. The bidders are, therefore, advised to mark ₹ 0/- (Rupees Nil) in BOQ line item C. They should also read the BOQ line item A as "Infrastructure at DC and DR including 05 years warranty".
	3.	The earnest money deposit has been revised to ₹ 20,00,000/- (Rupees Twenty Lakh for each schedule).
	4.	All the orders, circulars and notifications of The Government of India, Government of Himachal Pradesh, CVC, GFR etc. for public procurement like, those related to relaxations for MSMEs / Startups etc., Land border clause, Make in India or any other relevant issue shall be applicable to this bid.
	5.	Payment schedule modified as: 4.10.1. No payment will be made in advance for any supplies under this invitation for bid. 4.10.2. 70% of the total payment due (exclusive of annual maintenance charges, AMC, etc.) shall be released by the Bank upon successful delivery of equipment / software and raising of relevant invoices thereof. 4.10.3. Remaining 20% of the payment shall be released by the Bank upon successful commissioning after report has been issued by the Technical Committee / Consultant / concerned users within one month from the date of raising of relevant invoices thereof. 4.10.4. Remaining 10% of the payment shall be released by the Bank after 3 months of commissioning. 4.10.5. Operation and Maintenance charges shall be released by the Bank on quarterly postpaid basis upon rendering satisfactory services to the Bank and raising relevant invoice thereof by the vendor. The AMC for the supplies for the period after the warranty will be payable on quarterly basis on post-paid basis within one month of raising of relevant invoices thereof after making deductions for non-performance/downtime and other penalties imposed, if any. The Bidder may, however, prefer to raise invoice in advance also, though the payment shall be made strictly on post-paid basis.
	6.	The cost of Document is ₹ 5,000/- (Rupees Five Thousand Only) which needs to be remitted offline in the form of Cheques / DD (scanned copy should be uploaded online on e-tendering portal) along with the Proposal as directed in the Document. Hardcopy submitted to the Bank.
	7.	Earnest Money shall be deposited offline in the form of BG / Cheques / DD (scanned copy should be uploaded on e-procurement portal https://hptenders.gov.in/) as directed on the portal of the Government of Himachal Pradesh with the bid. The applicable payable amount is ₹ 20,00,000/- (Rupees Twenty Lacs only).
	8.	The specifications of Top of Rack Switch amended as: **Solution Requirement** The Switch should support non-blocking Layer 2 switching and Layer 3 routing. There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 inbuilt level of redundancy. **Hardware and Interface Requirement** Switch should have the 48 x 10G SFP fiber ports and should have 6 x 40G/100G QSFP28 ports. All the required optics should be provided. Switch should support minimum non-blocking full duplex switching capacity.

		Certification The Switch should be EAL 3 / NDPP / NDcPP certified under Common Criteria.
	9.	The bid submission and bid opening dates revised as follows: Last date of bid submission: July 01, 2023 (Saturday) at 2:00 PM Date of Technical Bid opening: July 01, 2023 (Saturday) at 3:30 PM
	10.	Details of the locations of the Bank are added as Annexure A.2 at page 62.