H.P. STATE ELECTRONICS DEVELOPMENT CORPORATION LTD.
(A Unit of H.P. Government Undertaking)

Request for Proposal
For
Supply, Installation & Commissioning of Firewall & Wifi Network Accessories in High Court of Himachal Pradesh

Tender No. HPSEDC/WiFi-HighCourt/2K23-5026

H.P. STATE ELECTRONICS DEVELOPMENT CORPORATION LTD.,
1st FLOOR, I.T BHAWAN, MEHLI, SHIMLA-171013, H.P.
Tel. Nos.: 0177-2623259, 2623043, 2623513.
Email: hpsedc@hpsedc.in

Definitions:

AMC:	Annual Maintenance Contract
BG:	Bank Guarantee
DD:	Demand Draft
EMD:	Earnest Money Deposit
FDR:	Fixed Deposit Receipt
GoLive:	is the date of commissioning of the project
OEM:	Original Equipment Manufacturer
PBG:	Performance Bank Guarantee
SLA:	Service Legal Agreement
TAC:	Technical Assistance Centre
Wi-Fi:	Wireless Fidelity
SIEM:	Security Information and Event Management
NMS:	Network Monitoring System
SDN:	Software Defined Network

1. **Disclaimer:**

All information contained in this RFP document provided/clarified is in the good interest and faith. This is not an agreement and this is not an offer or invitation to enter into an agreement of any kind with any party. Though adequate care has been taken in the presentation of RFP document, the interested firms shall satisfy itself that the document is complete in all respects. The information published in this document is not intended to be exhaustive. Interested respondents are required to make their own enquiries and assumptions wherever required. Intimation of discrepancy, if any, should be given to the specified office immediately. If no intimation is received by this office by the date mentioned in this document, it shall be deemed that the RFP document is complete in all respects and firms submitting their bids are satisfied that the RFP document is complete in all respects. HPSEDC reserves the right to reject any or all of the applications submitted in response to this RFP document at any stage without assigning any reasons whatsoever. HPSEDC also reserves the right to withhold or withdraw the process at any stage with intimation to all who have submitted their applications in response to this RFP. HPSEDC also reserves the right to change/modify/amend any or all of the provisions of this RFP without assigning any reason. Any such change would be communicated to the tenderers by posting it on the official website hptenders.gov.in. Information provided in this document is confidential to HPSEDC and shall not be used by the respondent for any purpose, distributed to, or shared with any other person or organization.

2. Introduction:

HPSEDC intends to establish a manageable wireless network with latest technology of higher throughput and scalability at specified locations in High Court Premises.

3. Notice Inviting Bid:

Sr. No.	**Subject**	**Description**
1.	Bid Inviting Authority	Managing Director, HPSEDC
2.	Requirement	Selection of System Integrator for Supply, Installation and Commissioning of Wireless

		(Wi-Fi) Network at specified locations in High Court Premises
3.	Bid Evaluation Criteria (Selection Method)	Least Cost Based Selection (LCBS)(L1)
4.	Correspondence address	Managing Director, HPSEDC, 1st Floor, IT Bhavan, Mehli, Shimla -171013 E-Mail-id: hpsedc@hpsedc.in
5.	RFP Name	Supply, Installation and Commissioning of Wireless (Wi-Fi) Network at specified locations in High Court Premises
6.	RFP reference no.	HPSEDC/WiFi-HighCourt/2K23-5026
7.	Pre-bid meeting	**Already held on 10/01/2024**
8.	Bid Submission Start Date	**27/08/2024 till 2:30 PM**
9.	Last date for receipt of bids online	**09/09/2024 at 02:30 PM**
10.	Date for Pre-Qualification and Technical bid opening online	**10/09/2024 at 02:30 PM**
11.	Date of Technical presentation by Bidders	**Will be notified to qualified bidders via e-Mail**
12.	Details to be submitted	The Tender process shall be done using e-tendering solution of GoHP at www.hptenders.gov.in The online bid submission shall comprise of the following: a. Checklist as provided in **Annexure-1**. b. Proof (Board resolution/ Power of attorney) stating that the person signing the bid is an authorized representative of the bidder. c. Proof of Submission of EMD. d. Online Technical and Financial bid The bids submitted by Post/telex/telegram/fax/e-mail etc. shall not

		be considered. No correspondence will be entertained on this matter
13.	Language of proposal	Proposals shall be submitted in **English.** If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the Bidders. For purposes of interpretation of the Proposal, the English translation shall govern. It shall contain no inter-lineation or overwriting, except as necessary to correct errors made by the bidder itself. Any such corrections must be initialed by the person (or persons) who sign(s) the proposals. An authorized representative of the bidder shall initial all pages of the proposal. The representative's authorization should be confirmed by a written letter of authorization accompanying the bid. Please Note that prices should not be indicated in the Eligibility Criteria/Technical Proposal but should only be indicated in the Commercial Proposal. The bid shall be rejected if found any prices indicated in Eligibility Criteria/Technical Proposal. All the pages of the proposal must be sequentially numbered and must contain the list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bid Conditional proposals in response to the RFP are liable to be rejected

14.	EMD details	The Bidders shall furnish, Earnest Money Deposit **(EMD) of 4 Lacs.** DD / EMD may be submitted through RTGS in HPSEDC A/c: (050010200006521, IFS Code: UTIB0000050, Axis Bank, SDA Complex, Shimla-9, HP.) Receipt/Copy of the demand draft/RTGS should be uploaded. EMD Fees shall be submitted by each bidder. The EMD can be scanned and uploaded on e-tendering portal. Meanwhile actual EMD must be send either by hand or through registered post and must reach this office on or before opening of Technical Bid. The bidder would be disqualified in the pre-qualification process if the EMD is not submitted before the last date & time specified for submission of online bids. Unsuccessful Bidder's EMD (bid security) will be discharged / returned as promptly as possible as after the award of the contract to the successful bidder. No interest will be payable by HPSEDC on the amount of the Bid Security. The bid security may be forfeited: 1 If a Bidder withdraws its bid or increases its quoted prices during the period of bid validity or its extended period without the explicit consent of the department, if any; or 2 During the whole process, if prospective/ successful Bidder indulges in any such

		deliberate act as would jeopardise or unnecessarily delay the process of evaluation and finalisation of offer. 3 Violates any of such important conditions of this document or indulges in any such activity as would jeopardize the interest of the Client. 4 In the case of a successful Bidder, if it fails within the specified time limit to: a Sign the Agreement in accordance with the conditions of this document or, b Furnish the required Performance Bank Guarantee(5% of the total value of supply) The decision of the Client regarding forfeiture of bid security shall be final & shall not be called upon question under any circumstances
15.	Date and time of Financial Bid Opening	Will be notified later to the technically qualified bidders.
16.	Bid Validity	180 days from the bid submission deadline.

4. Objective and Scope of Work:

In order to create IT infrastructure, HPSEDC plans to set up Wireless Networking infrastructure using state of the art networking equipment, Access Points, Integration at High Court Premises.

The following summarizes the scope of work.

A. To implement Wi-Fi Networking at specified locations in High Court of H.P.
B. To supply, install and commission all the components mentioned as per the technical and financial bid.
C. Successful bidder will be responsible to rollout the Wireless Network including, but not limited to user creation/ deletion/ updation/ provisioning/ tracking/ security/overall Wi-Fi Network Management and hand over to user department.
D. Successful bidder to provide detailed connectivity diagram (Physical and Logical) including: Raceways/pathways diagram, heat maps, Cable and fibre pathing details, Naming and labeling details, Cable Scanning and test results.

E. Successful bidder will carry penta scanning of each and every node of the WiFi Network.

5. General Terms and Conditions

1. The Bids under Two Bid System will consist of two parts as per following details:

i) Technical bid consisting of all technical details along with terms and conditions and EMD in the form of Demand Draft/FDR issued from any nationalized/Scheduled Commercial Bank in favor of the Managing Director, HPSEDC.

ii) Price Bid indicating price for the items/services mentioned in Financial Bid as per the BOQ mentioned herein.

In Stage one, only the technical bids shall be opened and evaluated. In Stage two, the price bids of only the technically qualified and acceptable offers will be opened, for further evaluation.

iii) The documents referred in Checklist and its Annexures thereof of this tender forms the technical bid evaluation criteria. All documents pertaining to the same as mentioned therein may be signed and stamped by the bidders and uploaded as technical bid on e-Tendering portal.

iv) The successful bidder will have to deposit 5% of the total value of supply as the performance security in the form of FDR or Bank Guarantee duly pledged in favor of Managing Director, HPSEDC, which will be returned after completion of the warranty period or will be adjusted in case of violation of terms & conditions laid down in this tender.

v) Conditional offer will not be accepted.

vi) It will be the sole responsibility of the bidder(s) that its bid should be uploaded on time on e-tendering portal.

vii) Necessary corrigendum(s), if required, will be issued at any stage. Any corrigendum will be published on our website https://hpsedc.in/tenders/ and also on www.hptenders.gov.in. Bidder(s) must be in touch with aforementioned websites for corrigendum (s). it will be sole responsibility of the bidder(s) that they will go through the corrigendum(s) published, if any, and submit its tender accordingly.

viii) The compatibility of all the networking components is the essence of this tender for efficient working of the network, hence bidders shall essentially quote all active components of one make for Wireless network. Any deviations in this matter will subject to disqualification. Similarly, bidder has to quote all the passive

components like optical fibre, CAT 6A or similar cable, LIU's, Fibre Patch Cords, Patch Panels, RJ-45 connectors of the same make as per Tender Specifications.

ix) Successful Bidder to provide Heat maps as a part of Wi-Fi Survey before start of actual work.

x) No part shipment/transshipment/third party shipment shall be acceptable.

xi) All pre bid queries regarding the tender must be submitted to email ID hpsedc@hpsedc.in on or before **05.12.2023 till 2:00 PM**.

xii) Minimum warranty period for each equipment/instrument should be for a period of 05 years from the date of delivery.

xiii) In case any manufacturing defect arises in equipment, it should be replaced within four working days.

xiv) In the event of goods not being in accordance with specification or the conditions of the contract or failure by the bidder to perform services as outlined in the Tender/bid document, HPSEDC reserves the right to cancel the contract at any stage.

xv) Validity of the quoted offer should cover the period of completion of the project. Offers without such validity need not to bid.

xvi) All information in the Tender/Bid should be in English language and each page of the Tender/Bid Document should be signed and stamped by the Bidder as a token of acceptance to terms and conditions.

xvii) Bidders should quote for all accessories which are either part of an item or are necessary for proper functioning of that item. Thus, for accessories of individual items, HPSEDC shall not pay anything separately and if the functioning of any item is not proper or does not function at all, HPSEDC shall have the full right to deduct complete payment for that item(s).

xviii) The successful bidder shall have to sign an agreement with HPSEDC/High Court of H.P. to comply with all rules, regulations, Laws and byelaws enforced by the State Government and High Court of H.P.

xix) It shall be the responsibility of the successful bidder to make an inventory of all the supplied materials upon its arrival at the customer's location and inform of missing components, if any.

xx) All passive cabling work whether it is fiber, UTP, Patch Panels, Racks Patch Cords etc. should be done neatly and with proper tagging. Entire cabling should be structured and aesthetically implemented.

xxi) Successful Bidder must have a local office presence in H.P. or arrange the same within a period of two months of issuance of work order.

xxii) Bidder must not have been blacklisted by any State/Central Government Department. An undertaking in this effect may be submitted.

xxiii) Participating in this tender would mean that bidder is accepting all terms and conditions of this tender document.

xxiv) All legal disputes, arising if any, would be settled under jurisdiction of High Court of H.P. Arbitration shall be only in the state of H.P.

6. Special Terms and Conditions

a. TERMINATION BY DEFAULT

HPSEDC may, without prejudice to any other remedy for breach of contract, by written 30 days' notice of default sent to the Successful Agency, terminate the Contract in whole or part. If the Successful Agency fails to deliver any or all of the systems within the period(s) specified in the Contract, or within any extension thereof granted by the purchaser pursuant to conditions of contract clause or if the Successful Agency fails to perform any other obligation(s) under the contract. In the event that HPSEDC terminates the Contract in whole or in part, pursuant to the conditions of contract clause, it may procure, upon such terms and in such manner, as it deems appropriate, systems or services similar to those undelivered, and the Successful Agency shall be liable to pay the HPSEDC for any excess costs for such similar systems or services. However, the Successful Agency shall continue the performance of the Contract to the extent not terminated.

b. All the items are to be quoted in Indian Rupees.

c. All prices quoted shall be inclusive of all taxes etc.

d. The bidder must clearly mention the make, model & enclose relevant datasheet/brochures along with requisite certificates of products as per technical specifications as mentioned in technical specification annexures.

e. Payment terms will be as follows, subject to the successful Audit Report as decided by HPSEDC.

i) 60% Payment of overall bid shall be processed at the time of delivery and subject to Bill of Material (BOM) Verification by High Court of H.P.

ii) 20% of payment of overall bid value shall be made successful installation and commissioning and completion.

iii) Remaining payment shall be made quarterly in 12 equal installments after Go-Live and subject to the satisfactory functioning of the network as per scope of the project.

f. HPSEDC may decrease or increase any active or passive component or both and make a commensurate adjustment in the corresponding service components while issuing work order or at a later stage. HPSEDC shall decide to add or drop any item at any stage of the tender process or on award of purchase order to successful bidder. Bidders are advised to quote competitively on each and every line item of the financial bid.

g. Delivery Schedule: The material delivery has to be done in four weeks at High Court of H.P. premises from the release of work order and complete installation has to be done within six weeks from the date of release of Work Order.

h. Warranty/Guarantee: The equipments supplied and installed shall be guaranteed by the Successful bidder for minimum period of five years with regards to quality of material, workmanship, performance, efficiency, installation, etc. Defects developed in the system within guarantee period, shall be rectified by the successful bidder at his own expense promptly within 24-48 hours. Bidder shall provide warranty from OEM for 5 years (5 years' warranty from bidder on legal format for whole solution).

i. The Passive quantity mentioned in the Tender/Bid is only indicative one. HPSEDC reserves the right to increase/decrease/remove any/all quantities while placing the order. All passive components will be paid on actual basis.

j. Any work not covered under this contract which may be essentially required for the completion of job (to the satisfaction of High Court of H.P.) shall be carried out by the successful bidder as extra item with prior approval of HPSEDC for which payment shall be made separately at reasonable rates decided by HPSEDC.

k. In case of failure, the specific penalties, if any, shall be imposed by Managing Director, HPSEDC.

l. EMD shall be released after receiving the PBG and signing the contract.

m. Warranty means smooth and regular uninterrupted functioning of the solution.

n. At any time, prior to deadline for submissions of bids, the procuring entity may for any reason, whether on its own initiative or as result of a request for clarification by a bidder, modify the bidding document by issuing an addendum/corrigendum in accordance with provisions below.

o. In case, any modification is made to the bidding document or any clarification is issued which materially affects the terms contained in the bidding document, the procuring entity shall publish such modification or clarification in the same manner as the publication of the initial bidding document.

p. In case a clarification or modification is issued to the bidding document, the procurement entity may, prior to the last date for submission of bids, extend such time limit in order to allow the bidder sufficient time to take in to account the clarification or modification, as the case may be, while submitting their bids.

q. Any bidder, who has submitted his bid in response to the original invitation, shall have the opportunity to modify or resubmit it, as the case may be, within the period of time originally allotted or such extended time as may be allowed for submission of bids, when changes are made to the bidding document by the procuring entity; provided that the bid last submitted or the bid as modified by the bidder shall be considered for evaluation.

r. Bidder shall be responsible to provide all the electrical equipments (like wires, pipes, MCB, switches etc.) that would be required to complete the project without any extra cost.

FORCE MAJEURE:

Force majeure shall mean any event or circumstances or combination of events or circumstances that materially and adversely affects, prevents or delays any party in performance of its obligation in accordance with the terms of the Agreement , but only if and to the extent that such events and circumstances affected party's reasonable control, directly or indirectly and effects of which could have prevented Good Industry Practice or in the case of the construction activities through reasonable skill and care through the expenditure of reasonable sums of money.

Any events or circumstances meeting the description of the Force Majeure which have same effect upon the performance of any contractor shall constitute Force Majeure with respect to the Vendor.

The parties shall ensure compliance of the terms of the Agreement unless affected by the Force Majeure events.

If a Force Majeure situation arises, the supplier/selected bidder shall promptly notify HPSEDC in writing of such conditions and cause thereof within 15 days of occurrence of such event. Unless otherwise directed by HPSEDC, the supplier/selected bidder shall continue to perform its obligations under the contract as far as reasonably practical.

If the performance in whole or part or any obligation under the contract is prevented or delayed by any reason of Force Majeure for a period exceeding 60

days, either party at its option may terminate the contract without any financial repercussion on either side.

7. Checklist

To ensure that your offer submitted to HPSEDC is complete in all respects, please go through the following checklist & tick mark for the enclosures attached with your offer:

Sr. No.	DESCRIPTION	DOCUMENTS REQUIRED	YES /NO	PAGE NO.
1.	General information about bidders as per Annexure I and the documents thereof	Annexure I and the documents thereof		
2.	Earnest Money Deposit	Demand Draft/FDR of Rs. 4 Lakhs		
3.	Letter of Proposal-Form 1	Letter of Proposal; as per template provided (Form 1)		
4.	Form 2	Technical Compliance as per detailed specifications of this Tender. Affidavit duly attested by Oath Commissioner.		
5.	Compliance and details on Annexure I- General Information about Bidder	Documentary Proof as per Annexure I		
6.	Compliance and details on Annexure II- Bidder and OEM Compliance	Documentary Proof as per Annexure II		
7.	Compliance and details on Annexure III	Documentary proof of SLA as per Annexure III		
8.	Local Office in Himachal Pradesh	a self-certified letter by an authorized signatory. In case, the bidder does not have an office, it has to set up its office for which declaration should be submitted.		
9.	Blacklisting	A self-certified letter by Authorized Signatory of Company/firm. In case of Consortium, all partners must submit a separate self-certified letter by Authorized Signatory.		
10.	Brochures/Catalogues	Product Catalogue sheets or equipment brochures clearly mentioning the model.		
11.	Technical Bid in Separate Sealed Envelope-Annexure I to Annexure VII Compliance.	Signed copy of the entire Tender and Annexure I to Annexure VII Compliance		
12.	Financial Bid in a separate Sealed Envelope- Annexure VIII	Annexure VIII to be placed in financial Bid of tender		

FORM 1: Proposal Letter

To

Managing Director,
HPSEDC, 1st Floor,
IT Bhavan, Mehli, Shimla -171013

Sir,

Having examined the Bid Documents, the receipt of which is hereby duly acknowledged, we the undersigned, offer to execute the Wi-Fi Networking works in conformity with the said Bid Documents and schedule of prices attached herewith as made part of this Bid.

We undertake, if our Bid is accepted, to complete the works within the specified period as per the Bid Document.

We also undertake that we accept all the terms and conditions of this Tender.

Until a formal contract is prepared and executed, this Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding contract between us.

We undertake that in completing for and if the award is made, in executing the above work, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act, 1988".

We acknowledge that we will complete the said project in all respects and also provide best of the support. We also undertake to put required manpower for smooth functioning of the setup for 03 years post execution of project.

Further we certify that our organization is not blacklisted by any Govt. Deptt.

Dated:
Place:

Authorized Signatory of Bidder with Company Stamp

FORM 2: Technical Compliance as per detailed specifications of the Tender

(Affidavit duly attested by Oath Commissioner)

To

Managing Director,

HPSEDC, 1st Floor,

IT Bhavan, Mehli, Shimla -171013.

Sir,

Having examined the Bid Documents of tender bearing no. HPSEDC/WiFi-HighCourt/2K23-5026, dated 08-08-2024, the receipt of which is hereby duly acknowledged, we the undersigned, offer to execute the Networking works as per the specifications mentioned in this tender.

We undertake that the Bill of material supplied as mentioned in Annexure V are fully Compliant with the detailed specifications of corresponding items from Annexure IV of this tender. Any non-compliance on technical specification or any other non-compliance of scope of work and terms and conditions of this tender will lead to cancellation of work order, blacklisting of our company, forfeiting of EMD submitted and a penalty of Rs.20 Lakhs.

Dated:

Place:

Authorized Signatory of Bidder with Company Stamp

Annexure- I

General Information about the bidder

1.	**Name of the Bidder**	
2.	**Postal Address**	
3.	**Telephone/Fax No.**	
4.	**eMail Address & URL**	
5.	**Type of Company** Attach Proof of Company Registration along with a copy of the Partnership Deep/Article Of Association and Memorandum of Understanding	
6.	**Name and designation of the representative** of the bidder to whom all references shall be made to expedite technical coordination.	
7.	**Amount and reference of EMD**	
8.	**Financial capacity of the Company/firm** (Attach copies of IT returns of Balance Sheets for last two years)	
9.	**Name and address of the Indian/Foreign collaborator(s) if any**	
10	**PAN/TAN Number** **(**A copy should be enclosed**)**	
11.	**GST Number**	

ANNEXURE-II: Bidder and OEM Compliance

S. No.	DESCRIPTION	DOCUMENTS REQUIRED	YES/NO	PAGE No.
1.	The bidder should be a registered Company/Organization/MSME with Government with Valid GST no. and PAN No.	GST Registration certificate and PAN Card		
2.	The Bidder should submit the Manufacturers Authorization Form (MAF) from the respective major OEMs.	Manufacturers Authorization Form (MAF) of One Page from each OEM.		
3.	The Bidder must be a profit making Company/Organization from last 5 years	Documentary Proof duly attested by registered CA..		
4.	Switches and Access Points should be from the same OEM to have single TAC for Active Components. Passive Components should be from same OEM.	Documentary Proof		
5.	OEM should have presence in India at least from last five years and making no losses in Networking business in last 5 years.	Documentary Proof		
6	the Bidder should have a minimum turnover of Rs.2 Crores in last three years	Documentary Proof duly attested by registered CA		
7.	Bidder/OEM must have executed similar work in any State/Central Government Departments/Government Agencies/PSU in last three years	Purchase Orders and completion Certificate from Government Departments/Government Agencies/PSU.		
	At least one project of Wireless Networking with work order of the value of Rs.1 Crore or more in any State/ Central Government Departments/Government Agencies/PSU; or Two Projects of Wireless Networking with work order of the value of 60 lakhs or more any State/ Central Government Departments/Government Agencies/PSU			
8.	Warranty and support from OEM for 5 years (Hardware/ Software) whole solution	OEM Certificate and 5 years warranty certificate from bidder on legal format on whole solution.		

Annexure-III-SLA

I. Bidder will be responsible for operations and maintenance for a period of three years.

II. For the purpose of measurement, "Downtime" or "Fault duration" constitutes any period of time during which the network connection is not useable for Data, Voice & Video. Causes of downtime include:

   a. Network connection equipment failures, supplied by Bidder.
   b. Process failure.
   c. Local loop failure in cables.
   d. Access Point, Core Switches & Access Switch
   e. Any failure in the entire solution provided.
   f. Cable fault in the network e.g. LAN cable, internal OFC Patch cords, patch panel etc.

III. All changes requests will be routed to Bidder for next three years and will be taken care by Bidder as a part of warranty with zero cost.

IV. Successful bidder to depute at least one networking resource, with more than three years of networking experience, for day to day operations and changes in Network for three years, without any cost implications.

V. Successful bidder will provide one-week training to designated team on entire setup of this project.

VI. Any spare replacement will be completed in a maximum of two working days for 5 years after completion of implementation phase. Any deviation on the part of successful bidder will attract a penalty of Rs.500/- per day.

VII. The successful bidder shall take immediate action to carry out any rectification work and restore the installation to its normal operating conditions upon receipt of the complaint from the Central Project Coordinator for a period of three years after installation of networking setup. If no action is taken to carry out the repairs within 24 hours upon lodging the report, the High Court of H.P. reserves the right to engage a third party to carry out rectification works with all the costs and expenses charged to the successful bidder. At the same time, bidder will attract a penalty of Rs.500 per hour for any non-compliance.

VIII. This SLA will be a part of agreement with further additions as deemed necessary by HPSEDC.

Annexure IV (Scope with Technical Specifications)

HPSEDC plans to set up Wireless (Wi-Fi) Networking infrastructure using state of the art networking equipment, Access points, Integration at **High Court Premises.**

The following summarizes the scope of work.

A. To Implement Wireless (Wi-Fi) Networking at **High Court of H.P.**

B. To supply, install and commission all the components mentioned as per the technical and financial bid and to carry out the work besides integration with existing IT Infrastructure (i.e. 1 x Router , 2 x 2Mbps Leased Line Modem, 1x 100Mbps Leased Line, 8 x 8Port 10/100/1000Mbps Layer2 Switches, 7 x 24 Port 10/100 Mbps and 10/100/1000 SFP, 1x CISCO Catalyst Switch Layer 3, 5 x Layer 2 Switches (Dlink), 1x Cisco Catalyst 2960 24 Port, 9xCisco Catalyst SG 200 24 Port, 9 x Dlink DES 1024) and access through NICNET connectivity available at High Court of H.P.

C. To supply, install and commission Intra building STP CAT6 A/UTP/ Fiber structured cabling Network as per BOQ and anything over and above as per actual need at the time of implementation.

D. Detailed Specification of Components needed as per Annexure IV.

E. Successful bidder will be responsible to roll out the wireless (WiFi) Network including, but not limited to user creation/deletion/updation/provisioning/ tracking/security/overall Wireless Network management and handover to User Department.

F. Successful Bidder to provide detailed connectivity diagram (Physical and Logical) including: Raceway/pathway diagram, heat maps, Cable and Fiber patching details, Naming and labeling details, Cable scanning and test results.

G. Successful Bidder will carry penta-scanning of each and every node of the Wi-Fi Network.

S. No.	Scope of Work with further details

1	**Campus Design Scope of work**
i.	Campus design must be based on routed access i.e. using L3 at access to avoid any STP or broadcast/flood related issues
ii	All switches i.e. Access switches and Core switches need to be provided with all software license from day-1 to support functionality mentioned in RFP specification
iii	Campus solution should have network automation tool for zero touch provisioning building network and host inventory topology creating network segment and network access policy software image update troubleshooting end to end connectivity getting OEM update on security update/advisory end of sale/end of life update etc.
iv	Campus solution should have capability to provide user mobility on wired network (Users moving from one floor to another floor) without changing ip address or vlan. Vendor needs to provide details on how they are going to achieve it with their solution.
v	There has to be end to end logical separation (including routing table) between campus data users and guest/contractors.
vi	It should possible to create micro segmentation between floor users where we should able to restrict communication between users on the same segment/vlan and communication between users will only be allowed based on policy. Vendor needs to provide details on how they are going to achieve it with their solution.
2.	**Campus Access control solution**
i.	Campus solution should include secure campus access and secure guest access components (software and license) from day-1. It should allow campus access based on user id and password, MAC address, certificate etc. It should allow contractors and guest to bring their devices and access authorized resources in secure way It should able to provide visibility on connected users, devices types, how they are connected etc. It should allow password management for guest in automated, approval based access It should possible to send guest password on email and SMS It should allow to provide guest/contractor access based on hours, days and weeks
ii.	Proposed solution should integrate with existing IT infrastructure and access through NICNET Connectivity that supports industry standards such as 802.1x, CoA, WebAuth/Web Redirect
iii.	Solution should support wide range of authentication protocols, including PAP, MSCHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAPFlexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS).

iv.	Secure access software needs to be provided for minimum 1000 end devices license including 500 guest access/BYOD license
v.	Hardware/Virtual appliance in High availability (HA) needs to be provided to run secure access software
vi.	Secure access software should support local user database, active directory integration
vii.	Campus access control solution should able to share contextual information with visibility and threat analytics solution and should support bidirectional context sharing
3.	**Campus Visibility and threat analytics solution**
i.	Campus solution should include network visibility and threat analytics solution based on flow records. It should allow visibility on user traffic flow, type of device, top talkers, user to user communication detail like application, ports etc., traffic anomalies based on campus traffic analysis, alarm generation based on traffic anomalies, highlighting top attackers, top victims etc.
ii.	The solution should detect common events like Scanning, Worms, Unexpected application services (e.g., tunneled protocols, backdoors, use of forbidden application Protocols), Policy violations, password detection mechanism (like brute-force)etc.
iii.	The solution should detect applications running on non-standard port numbers. The solution should display traffic profiles in terms of packet rate.
iv.	The solution should support detection methods/fingerprints for Phishing, Botnets, Malware, Spyware, DDOS , Worms , Virus , protocol anomalies (Internal , external) Connections to bad reputation Nations and Dark IP .
v.	It should support netflow/sflow/jflow/IPFIX
vi.	The solution should be able to store full flow data for long-term for forensic purpose
vii.	The solution should be able to visualize malware propagation behavior
viii.	Solution should have the ability to statefully reassemble uni-directional flows into bidirectional conversations; handling de-duplication of data and asymmetry
ix.	The solution should do Data Flow Analysis across all ports and services and not limited to data being transported via HTTP/HTTPS/SMTP/IMAP/POP/ SSH / telnet and other into and out of the network
x.	It should able to detect traffic anomalies in encrypted traffic
xi.	It should possible to isolate attacker or infected machines from network with integration with campus access control solution. Integration should be based on IETF standard driven framework

xii	The solution should be able to integrate with various SIEMs available in the market like RSA, Splunk, HP, etc
xiii	All hardware and software license for campus visibility and threat analytics solution.
4.	**General Requirement**
i.	It is desirable to have entire solution from single OEM
ii.	OEM offering switches, campus access control and visibility and threat analytics solution should have offices in India and 24x7x365 TAC support
iii.	Central controller should corelate logs collected from Network, AAA, DNS, DHCP etc. It should allow to view historical state of the network including the actual meta flows and user data collected on the network at any point of time for the last 7 days. The controller should provide actionable insight based on analysis of this information.
iv.	Network should send real time telemetry push data to central controller. This should not be based on non-real time polling based methods which are prone to loss of accuracy.
v.	Controller should provide information on overall network health of each floor of High Court and provide details on switch CPU, Memory, modules insights.
vi.	Controller should create network inventory and should poll devices in the network at periodic basis for inventory maintenance
vii	Controller should have tight integration with user policy engine to have visibility of user and device data on the network and push user policies from controller.
viii	Controller should automate network provisioning which includes zero touch provisioning, creation of network fabric, user authentication, authorization and access policy, Setting AAA, SNMP, DHCP, DNS servers etc.
ix	Controller should provide end to end path troubleshooting highlighting ingress and egress interfaces, ACL and QoS policy, packet drops etc.

Technical specifications

Sr. No.	Item
1	Dual Band WiFi 6 Access Points
2	Wireless LAN Controller For 5 Years
3	24 Port PoE Access Switch
4	24 Port Access Switch
5	24 Port Aggregration PoE Switch
6	24 Port Core Switch
7	Core Router
8	SFP modules, SM, 1Gbps
9	SFP modules, SM, 10Gbps
10	CAT 6 Cable

11	24 port Patch Panel
12	CAT 6 Patch cord 1m
13	CAT 6 Patch cord 2m
14	IO CAT 6, 1 Port
15	Fiber Optic 12F Cable
16	Information Outlet
17	Fiber Optic Patch cord SM, LC-LC, 3m
18	UTM Firewall
19	Fiber Optic Pigtail SM, SC, 3m
20	LIU 12F, 19" Rack Mountable, with couplers and accessories
21	LIU 24F, 19" Rack Mountable, with couplers and accessories
22	LIU 48F, Wall Mount, with couplers and accessories
23	19" 12U Rack
24	Termination of CAT 6 cable in IO Box
25	Termination of CAT 6 Cable on Patch Panel
26	PVC Conduit ISI Mark, 32mm / 40mm
27	In Building laying of UTP CAT 6
28	Fiber Optic Cable Termination
29	HDPE PLB Pipe, 32/26 mm
30	HDPE PLB Installation (Outdoor – Underground 1m, Soft Soil)
31	HDPE PLB Installation (Outdoor – Underground 1m, Concrete)
32	Project Management, Installation, Commissioning & Testing

WiFi 6 Access Points

Building	Floor	Section/Unit	No. of Access Points
Main Building	Basement	Record Room	1
	Ground Floor	O&A Branch & Establishment Branch	2
		GAD Branch	2
		Outside GAD Branch	1
		Judges Library	1
		Record Room	1
	I Floor	Gallery(for covering all rooms)	4
		Protocol Officer	1
	II Floor	Bar Room	2
		Reception	1
	III Floor	Registrar (Administration) Room	1
		Court Room 08	1
		Court Room 08 Chamber	1
		Secretary Room Court 08	1
		Staff Room	1
		Registrar (Rules) Room	1
		Registrar (Vigilance) Room	1
		Vigilance Branch	1
	IV Floor	PA Room	1
		Court Room 06	1
		Court Room 06 Chamber	1
		Secretary Room Court No. 6	1
		Court Room (Vacant)	1
		Court Room(Vacant) Chamber	1
		Secretary Room	1
		Court Room 07	1
		Court Room 07 Chamber	1
		Secretary Room Court 07	1
	V Floor	PA Room	1
		Court Room 05	1
		Court Room 05 Chamber	1
		Secretary Room Court 05	1
		Court Room 04	1
		Court Room 04 Chamber	1
		Secretary Room Court 04	1
		Court Room 03	1
		Court Room 03 Chamber	1
		Secretary Room Court 03	1
	VI Floor	Court Room (Vacant)	1
		Court Room (Vacant)Chamber	1
		Secretary Room Court(Vacant)	1
		Court Room 02	1
		Court Room 02 Chamber	1
		Secretary Room Court 02	1
		Court Room 01	1
		Court Room 01 Chamber	1
		Secretary Room Court 01	1
		Registrar General Chamber	1
		Confidential Branch	1
		CJ Court	2

	VII Floor	Judges Lounge	1
		Outside Judges Lounge	1
		Chief Justice Chamber	1
		CJ Secretariat	1
		Total	**61**
New Administrative Block	Ground Floor	Registrar Judicial Chamber	1
		Common Area Front (for all rooms)	3
		RSA Branch	1
		Common Area Back(for all rooms)	2
		FAO Branch	1
		CWP Section	1
		CWP OA Section	1
	First Floor	Computer Branch	2
		Civil Revision	1
	Second Floor	Auditorium	4
		Pantry	1
	Total		**18**

Additional one no. of Access point is required to cover black spot.
Total no. of WiFi Access Points= 61 + 18+ 1 = 80

LAN Switches

		Existing	Planned			
Building	Floor	Existing Switch Ports (Managed & unmanaged)	# Dual Band WiFi6 Access Points	#24 Port Access Switch	#24 Port POE Access Switch	#24 Port Aggregation POE Switch
Main Building	Basement	24	1	0	1	0
	Ground Floor	24+8	7	2	0	1
	I Floor	24+24	5	2	0	1
	II Floor	24+24	3	2	0	1
	III Floor	24+8	8	2	0	1
	IV Floor	24+8	10	2	0	1
	V Floor	24+24	10	2	0	1
	VI Floor	24	9	1	0	1
	VII Floor	24+8	8	2	0	1
		Total	**61**	**15**	**1**	**8**
New Building	Ground Floor	24+24+24+ 24+24+24	10	6	0	1
	First Floor	24+24+24+ 24+24+24	3	6	0	2
	Auditorium	24	5	1	1	0
		Total	**18**	**13**	**1**	**3**

Total No. Access Switches = 30
Total no. of Aggregation Switches= 11

Sr. No	Technical Specification for Wireless Access Point	Compliance (Yes/No)
	Make and Model:	
1.	Wireless AP fully IEEE 802.3 compatible on the Ethernet side and fully interoperable with IEEE 802.11a/b/g/n/ac/ax compliant equipment.	
2.	802.11ax specified for both downlink and uplink multi-user MIMO and Orthogonal Frequency Division Multiple Access (OFDMA) technology. Support 160MHz/80+80MHz to channels to double capacity.	
3.	Operation at 2.4GHz and 5GHz band to meet worldwide regulations (included DFS band).	
4.	AP should support Supports one 2.5GbE port and one 1GbE port. Support LACP or Static Link Aggregation. AP should be power ON by PoE or External power supply.	
5.	AP should have RJ-45/USB Console port	
6.	AP should support 4x4 11AX MU-MIMO, 2.4 GHz Data Rate: 573 Mbps (40MHz/1024QAM), 5 GHz Data Rate: 2402 Mbps (80MHz/1024QAM), Up to 1024 QAM on both 2.4GHz & 5 GHz bands, Supports 20MHz/40MHz/80MHz/80+80MHz/160MHz channels	
7.	AP should have 4x4 Internal antennas, Antenna Gain: 3dbi @ 2.4GHz; 4dbi @ 5GHz and Allows up to 250 wireless clients connected	
8.	AP Should have Plenum rated UL-2043, Reset Button for device reboot and Reset to Factory Default settings.	
9.	AP should Supports DHCP for dynamically obtaining network configuration in Managed Mode	
10.	Detection & Prevention, Rogue and Valid AP Classification	
11.	Operating temperature should be 0 degree Celsius 0 to +40 degree Celsius.	
12.	Certification: Wi-Fi CERTIFIED, EN55032, EN55024, EN61000-3-2, EN61000-3-3, EN60601- 1-2 (Medical electrical equipment), EN301489-1, EN301489-17, EN300328, EN301893, cUL+UL (UL/CSA 62368-1 + UL 60950-22), UL2043."	
13.	AP should supports enhanced security – WPA2/3-Personal & WPA2/3-Enterprise	
14.	Allows auto fallback data rate for reliability, optimized throughput and transmission range.	
15.	Should support up to 16 Virtual SSID's per radio. For each VAP, you can configure a unique SSID name, a default VLAN ID, a security mode, external RADIUS server information.	
16.	In standalone mode AP can be managed through Web GUI, CLI or SNMP.	
17.	Should supports of 802.1Q VLAN Tagging and Maximum of 64 Dynamic VLANs.	
18.	Should supports 802.1p Quality of Service (QoS) for enhanced throughput and better performance of time-sensitive traffic like VoIP and streaming.	
19.	Should support Wi-Fi Multimedia (WMM) for QoS and DSCP and Supports WMM - Power Save and 802.11e U-APSD - Unscheduled Automatic Power Save Delivery	
20.	Manually limit the number of simultaneous users per AP.	
21.	RADIUS (RFC 2865, 3580) - Supports authentication with RADIUS and Can configure up to 4 external RADIUS servers for failover	
22.	Should Supports Supports 802.11h, incorporating Dynamic Frequency selection (DFS) and Transmit Power Control (TPC)	
23.	AP should support Supports STP to prevent loops when using WDS (wireless bridge) links as redundant links to a distribution system.	

24.	Should have feature like airtime fairness and to encourage dual-band capable clients to connect to its 5GHz radio. Ensures that equal airtime is given to each client, providing increased performance even if slower devices are connected.	
25.	MAC filtering- Configure a list of MAC addresses to permit/deny access and Local or RADIUS database	
26.	Should have strong security with Extensible Authentication Protocol (EAP) - EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAP-GTC, PEAP-TLS, PEAP-MS-CHAPv2, EAP-Fast and EAP-AKA.	
27.	Station Isolation - Wireless Client associated with the same radio cannot detect each other.	
28.	Support Time Zone. The Time Zone can be selected. This is key when using SNTP to synchronize the system time. This also brings in support for Daylights Saving	
29.	Syslog (RFC 3164) - System Logs, Syslog Email Alert: Generates email messages based	
30.	The abbreviation of Link Layer Discovery Protocol for Media Endpoint Devices. Allow AP to exchange power information with PoE PSE.	
31.	Should support a list of MAC addresses to permit/deny access.	
32.	**Warranty:**	
33.	5 Years of Hardware Warranty	
34.	No repair products & replacement with New Box	
35.	**Note:-**	
36.	Wi-Fi AP should be supplied with the all necessary components like wall and ceiling mount bracket, Installation Guide, etc. and necessary software image file to fulfill all above mention feature set from day 1.	

Access Switch

Sr.No	Access Switch: 24 Port 1G copper and 4 x 10G SFP uplinks Ports	Compliance (Yes/No)
	Make and Model:	
1.	Should support IEEE 802.1Q VLAN encapsulation and up to 512 active VLANs per switch	
2.	Should support VTP or equivalent protocol to reduce administrative burden of configuring VLANs on multiple switches in turn eliminating the configuration errors & troubleshooting in secure manner.	
3.	Shall have minimum 8000 MAC Address support	
4.	Shall support 802.3ad link aggregation and 802.1s MSTP.	
5.	Should support DiffServ / TOS Marking & Policing	
6.	Shall have at least 4 Queues to differentiate and prioritize different applications (Voice / Video / Data)	
7.	Should Support for IGMP v1, v2 and v3 and IGMP Snooping	
8.	Shall have static route and RIP v1/v2 support from day one.	
9.	Should support IPv6 management with Neighbor discovery	
10.	Should support IEEE 802.1x to allow dynamic, port-based security, providing user authentication	

11.	Should support MAC Address Based Security on per port basis.	
12.	Should support IEEE 802.1x with an ACL assignment for specific identity-based security policies	
13.	Should support Port-based ACLs (PACLs) for Layer 2 interfaces allow application of security policies on individual switch ports	
14.	Should support SSHv2 , SNMPv3 and NTP/ SNTP to provide network security	
15.	Should support TACACS+ and RADIUS authentication	
16.	Should support image and configuration rollback	
17.	Should have Port and VLAN based Mirroring with support for mirroring to remote port/VLAN.	
18.	Management: Should support accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface	
19.	**Warranty and Support**	
20.	5 years hardware replacement warranty	
21.	Technical support using telephonic/chat, & email, & the provision of the latest firmware during the warranty period by OEM/SI.	

Spec-Access PoE Switch

Sr.No.	24 Port PoE Access Switch	Compliance (Yes/No)
	Make & Model	
1.	Switch Should Support 24 10/100/1000BASE-T PoE, 4 SFP ports and RJ-45 console port. All Gigabit Ethernet ports support IEC 61000-4-5 surge protection	
2.	switch should support Operating Temperature 0 to 40 °C (23 to 122 °F)	
3.	Switch Should Support Min. 56 Gbps Switching Capacity and Maximum 64 Byte Packet Forwarding Rate is 41.7 MPPS, 16K MAC address table.	
4.	The Switch support SNMP traps	
5.	Switch Should Support IEEE 802.3af & at compliance (for PoE ports) and 193W Power Budget.	
6.	Switch Should Support IGMP Snooping v1, v2 and MLD snooping v1/v2	
7.	Switch shall support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) & LLDP-MED.	
8.	Switch Should Support IEEE 802.3az Energy Efficient Ethernet (EEE) Power saving Technology, Power Saving by Link Status, Time-based PoE, Port shut off, Cable length detection Etc.	
9.	Switch Should Support 4K VLAN ID's, Min 256 static VLAN , Multicast VLAN and Auto Voice & Video VLAN	
10.	Switch Should Support Port Mirroring One to one/Many to One,	
11.	Switch should support Quality of Service (QoS), 802.1p, Strict, Weighted Round Robin (WRR), Bandwidth Control.	
12.	Switch Should Support IP interfaces, Static routing for inter-VLAN Communication	
13.	Switch should support Access Control List (ACL), Port Base, MAC Base, IP Based, L2 & L3 ACL (IPv4 and IPv6) ERPS sub-50 m protection and recovery or equivalent	

14.	Switch Should Support Security Features like Broadcast/Multicast/ Unicast Storm Control, Traffic segmentation, TLS, DoS attack prevention, 802.1X Port-based Access Control, Port Security, ARP Spoofing Prevention, DHCP Guard, IP-MAC, Port Binding, ARP Inspection, DHCP Snooping..	
15.	Switch Should Support 802.1X Authentication local/RADIUS database (IPv4 & IPv6), port-based access control, EAP, OTP, TLS, TTLS, PEAP and Support MD5 authentication	
16.	Switch Should Support features Cable diagnostics, IPv4 & IPv6 Inspection, SSH v2 feature, 802.3x Flow Control and HOL Blocking Prevention	
17.	Switch Should Support Management thru Web-based and CLI.	
18.	Switch Should Support SNMP v1/v2c/v3, SNTP, ICMP v6, IPv4/v6 Dual Stack, Dual image, Dual configuration	
19.	Switch should have EMI CERTIFICATE as per EN/FCC/IC/CE.	
20.	Switch should have SAFETY CERTIFICATE as per UL/ IEC/EN 60950	
21.	Switch should be supplied with the all necessary components like Power supply, Power cord, Console Cable, Rack-mount kit, Installation Guide, etc. and necessary software image file to fulfill all above mention feature set from day 1.	
22.	**Warranty** : 5 years comprehensive onsite warranty	

Specs-Agg Switch

Sr. No.	Specifications Aggregation Switches (Distribution Switch)	Compliance (Yes/No)
	Make & Model	
1.	Proposed Switch should have 24 10/100/1000BASE-T ports and 4 SFP+ ports	
2.	Switch should Support Internal/External Redundant Power Supply.	
3.	Switch shall have SD Card slot/USB/External flash for easy file store & restoration like firmware, configuration file, boot image, syslog etc	
4.	Switching Capacity should be 128 Gbps & Packet Forwarding rate should be 95 Mpps.	
5.	The Switch shall support Min. 16K Mac address	
6.	Switch should support Physical Stacking up to 8 units per stack. Stacking bandwidth should be up to 80G	
7.	Switch should support ARP, Proxy ARP and Gratuitous ARP.	
8.	The LAN switch shall have IEEE 802.1Q VLAN encapsulation and should support 4k Vlans.	
9.	It shall have support for Detection of Unidirectional links and to disable them to avoid problems such as spanning tree loops	
10.	It shall support 802.1v Protocol-based VLAN	
11.	Should support MAC based Vlans	
12.	Should support GVRP or equivalent, Private Vlan or equivalent, Subnet Vlan or equivalent, Voice Vlan and QinQ (port based qinq and selective qinq).	
13.	Multicast VLAN to allow multiple VLANs to receive the same multicast traffic	
14.	Should have 802.1D STP, 802.1w RSTP and 802.1s MSTP Spanning Tree Protocol and provide protection for Ethernet traffic in ring topology..	

15.	The Switch should have 802.1AX Link Aggregation Up to 30 groups per device	
16.	Port Mirroring One to one/Many to One, Flow based mirroring & VLAN Mirroring	
17.	The Switch shall have the intelligence to detect the loop occurring from the unmanaged network segment	
18.	Switch should support Static routing for IPv4 and IPv6, RIP for IPv4 and RIPng for IPv6, VRRP v2 & V3, OSPF,OSPF v3 and BGP4 from day 1	
19.	Switch should support PIM-SM, PIM-SSM, PIM-SMv6 and GVRP	
20.	IPv6 Tunneling: Tunnel types should be supported are Static, 6to4 and ISATAP	
21.	Should support DoS, ECMP, policy based routing, Route Redistribution support	
22.	Switch should support 802.1p priority queuing with 8 queues per port.	
23.	Queue Handling mode: WRR & Strict Mode, Strict + WRR and DiffServ	
24.	Granular Rate Limiting functions on per port & flow based to guarantee bandwidth in increments shall be as low as 8 Kilobits per Second.	
25.	Class of service shall be based on Switch port, DSCP, Vlan ID,TCP/UDP port, Protocol type,802.1p queues, IPv4/v6 address, IPv6 flow label & User defined packet content	
26.	Broadcast and Multicast traffic/storm control	
27.	Should support UDLD and DDM	
28.	IEEE 802.1X Port Based Access control and Host based Access control and Guest Vlan	
29.	It shall support RADIUS/TACACS+ authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.	
30.	It shall have IP-MAC-Port binding and Safeguard Engine	
31.	Switch should be able to authenticate and access control based on MAC and web (Http or Https)	
32.	BPDU Attack Protection, ARP protection, IP Source Guard, Dynamic ARP Inspection and DOS Attack Prevention	
33.	It shall support for SSHv2, SNMPv3 to provide network security by encrypting administrator traffic	
34.	Able to manage trough Web-GUI, Fully functional CLI interface and Telnet.	
35.	Should support sFlow for monitoring traffic in data networks, SNMP v1, v2c, v3 and SNMP Traps and RMON.	
36.	Switch should be EMI Certificates FCC, CE/CB and Safety Certifications cUL/UL, IEC	
37.	Switch should be supplied with the all necessary hardware accessories like Power cord, Rack-mount bracket, Installation Guide, etc. and necessary software image file to fulfill all above mention feature set from day 1.	
38.	Warranty : Three years comprehensive onsite warranty	

SPECS-CORE SWITCH

Sr.No.	Specifications Core Switch	Compliance (Yes/No)

	Make & Model	
1.	The Core Switch should be high-performance switches that feature high port density, routing, and ultra-low latency	
2.	Non-Blocking architecture. Switch should be EMI Certificates FCC, CE and Safety Certifications cUL/UL, CB.	
3.	Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software	
4.	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.	
5.	Switch should support VXLAN, ONIE / OpenFlow v1.3	
6.	Should support at least 48-port 1G/10G SFP+, 6-port 40G/100G QSFP28 Ports	
7.	Switch should support Virtual Switch Stacking / MLAG with VRRP for Switch level Redundancy"	
8.	All Switches and Fiber Modules should be from Same OEM	
9.	The Switch have 2.16Tbps Switching Capacity, and forwarding rate 1607.4Mpps, for Higher switching functionality	
10.	MAC Address Table - Min 32 K, MTBF - 90K hours Min	
11.	Min 4K static VLAN groups and Min 4K VIDs	
12.	Switch should support STP/MSTP/RSTP and ERPS/RRP	
13.	802.1AX Link Aggregation, Multi-Chassis Link Aggregation Group (MLAG)	
14.	IGMP & MLD Snooping, Multicast Table Size: Up to 16K, PIM-SM IPv4/IPv6, PIM-SSM	
15.	Port Mirroring, Flow Mirroring, RSPAN mirroring	
16.	The switch shall have hardware based forwarding for IPv4 & IPv6.	
17.	Following protocols shall be supported with IPV4: Static routing, PBR, RIPv2, OSPFv2, BGPv4, PIM, VRRP from day one, BGP, VRF	
18.	IPV6: PBR, Static routing, OSPFv3, BGP	
19.	The switch shall have Dual stack mode to run both IPv4 & IPv6, IPv4/IPv6 Routing Table - Min 16K	
20.	Shall support VRRP for IPV4 and IPV6	
21.	MAC and 802.1 X based Login must be available, Supports 802.1X NAP	
22.	MAC Address based Lockdown and Limited Learning	
23.	L2/L3/L4 IP based, Source port, destination port, MAC based, Time based	
24.	AAA using RADIUS must be available, Identity-driven Policy (VLAN/ACL/QoS) Assignment, Guest VLAN	
25.	Secure Web based management (On https) through NMS or Full featured CLI, TELNET Access.	
26.	SSH based management (SSH v2) or support UDLD	
27.	Serial console port, Alarm Port, USB Port, Management Ethernet port - Dedicated OOB port	

28.	The switch shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges	
29.	The switch should support SNMP V2c & V3 and RMONv1/ RMONv2 support or equivalent"	
30.	Syslog shall be supported with multiple syslog destinations.	
31.	Shall support Netflow/IPFIX/sflow for flow exports	
32.	Time synchronization using Network time protocol must be available	
33.	The switch shall have feature of backing up the configuration & restoring a backed- up configuration. Multiple Configuration files must be supported.	
34.	Config/image upload and download from TFTP/FTP server shall be available.	
35.	Switch should be supplied with the all necessary hardware accessories like PSU, Power cord (full load front-to-back AC PSUs - 2 Min), Stacking Cable (QSFP28 to QSFP28), Rack-mount bracket, Installation Guide, etc. and necessary software image file to fulfill all above mention feature set from day 1.	
36.	Power Supply & FAN - Switch should support Internal Hot swappable PSU and Field replicable FAN module.	
37.	Safety certification - The switch shall conform to IEC-60950/CSA60950/EN-60950/UL-60950 standard for safety requirements of information technology equipment.	
38.	Environmental conditions- The offered equipment must be able to operate in the following environmental conditions	
39.	Operating temperature: 0°C to 45 °C and Relative Humidity: 10% to 95% Non-condensing	
40.	Warranty : Three years comprehensive onsite warranty	

Specs

Sr.No.	Specs SFP	Compliance (Yes/No)
1.	**Make & Model:**	
2.	Description: 1GBASE-LR SFP Transceiver	
3.	Fiber Module should be Hot Pluggable, MSA Compliant and RoHS Compliant	
4.	Wavelength: 1310 nm	
5.	Fiber Module should support 10KM Distance	
6.	Certification - CE, FCC, UL, LVD, TUV, VCCI. (Should Enclosed with bid)	
7.	Warranty : Three years comprehensive onsite warranty	
	Specs SFP+	**Compliance (Yes/No)**

1.	**Make & Model:**	
2.	Description: 10GBASE-LR SFP+ Transceiver	
3.	Fiber Module should be Hot Pluggable, MSA Compliant and RoHS Compliant	
4.	Wavelength: 1310 nm	
5.	Fiber Module should support 10KM Distance	
6.	Certification - CE, FCC, UL, LVD, TUV, VCCI. (Should Enclosed with bid)	
7.	Warranty : Three years comprehensive onsite warranty	
	Optical Fiber Cable Specs	**Compliance (Yes/No)**
	Make & Model:	
1.	The Fiber should be 6 & 12 core OS2 Fiber Central -loose tube filled with Thixotropic jelly	
2.	The Fiber should follow Standards: ISO 11801, IEC 60793-1/60794-1- 2/60794-3-10 and ITU-T-REC G.652D	
3.	The Fiber should be with High quality Electro Chromium Coated Corrugated Steel tape (ECCS) and LSZH- Sheath	
4.	The Fiber Operating Temperature should be – 20 deg C to +60 deg C and Storage Temperature should be – 20 deg C to +60 deg C	
5.	The Fiber Max Attenuation ± 0.36 (db / km) @ Operational Wavelength 1310 nm and, ± 0.22 (db / km) @ Operational Wavelength 1550 nm .	
6.	The Fiber - type should be 9/125 / G.652D & Refractive Index should be 1.4674/1.4679	
7.	The value for Mode-filed/Cladding Diameter (um) 9.2 ± 0.4 and 125 ± 0.7	
8.	The Dispersion value <=3.5 <=18 (ps/(nm-km) and PMD value <=0.2 (ps/km) and Cable Cut-off wavelength <=1260 (nm)	
9.	Warranty : Three years comprehensive onsite warranty	
	Pigtail SM	**Compliance (Yes/No)**
	Make & Model:	
1.	Corning single-mode G652D,G657A,G657B	
2.	Cable Type:-0.9mm	
3.	Apex Offset <50um	
4.	Fiber Height +(-) 100nm	
5.	End-face Radius of curvature 7mm < R < 25mm	
6.	Working Temperature:- -40 oC ~ + 85 o C	
7.	Storage Temperature :- -40 o C ~ + 85 o C	

8.	Warranty : Three years comprehensive onsite warranty	
	LIU	**Compliance (Yes/No)**
	Make & Model:	
1.	Should be Rack Mount for 12, 24 & 48 Port and should be loaded.	
2.	Front-mounted cable saddles for jumper management	
3.	Can manage both splices and terminations	
4.	Preassembled shelves in multiple configurations	
5.	Rubber fiber slotted bracket built-in, metal splice shelf to protect the fibers	
6.	2 fiber spools built-in for 900µm tight buffered fiber storing	
7.	Capable of storing up to 3 meters of 900µm tight buffered fiber per adapter	
8.	Removable front and rear covers for better access to interior of LIU	
9.	Should be Single mode LC Type fully loaded.	
10.	Accessory kit consists of cable ties, mounting ear screws, and spiral wrap tube	
11.	Warranty : Three years comprehensive onsite warranty	
	Optical Fiber Patch Cord SM LC to LC Fiber LSZH Duplex Patch Cord (OS2)	**Compliance (Yes/No)**
	Make & Model:	
1.	Adopts high precision ceramic ferrule with good concentricity	
2.	Fiber corning single mode G652D,G657A,G657B	
3.	Cable Type 0.9mm	
4.	Mechanical specification Apex Offset :-< 50 um	
5.	Mechanical specification Fiber Height +(-) 100 nm	
6.	End-face radius of Curvature 7mm < R <25mm	
7.	Working Temperature :- -4 0 c ~ +85 o C	
8.	Storage Temperature:- 40 o C ~ + 85 o C	
9.	Length – As per requirement	
10.	Type -- LC-LC Duplex	
11.	Warranty : Three years comprehensive onsite warranty	

	Unshielded Twisted Pair Category 6 Cable	**Compliance (Yes/No)**
	Make & Model:	
1.	Category 6 Unshielded Twisted Pair 4 pair should be complied as per ETL verification program for compliance with ANSI/TIA-568.2-D standard and ISO 11801 Class E standards at swept frequencies up to 250MHz	
2.	4 twisted pairs separated by internal X shaped, full separator.	
3.	Conductor dia: 23 AWG	
4.	Insulation :POLYETHYLENE	
5.	Outer sheath: LSZH GREY- Single sheath	
6.	RIP CORD: YES	
7.	Sequential meter marking: YES	
8.	Temperature Rating: "-20° to +70°C	
9.	Filler Required: YES	
10.	Packing :305 Mtrs	
11.	Low Frequency Electrical Parametre	
12.	CONDUCTOR RESISTANCE: (DC) 93.8 OHMS/1000 MTR @20 Degree C. MAX.	
13.	RESISTANCE UNBALANCE :5%MAX	
14.	MUTUAL CAPACITANC: E 5.6 nF/100 mtrs Max.	
15.	CAPACITANC E UNBALANCE PAIR/GROUN D :330PF/100M MAX	
16.	Propagation Delay Skew :536 nS/100M	
17.	Nominal Velocity of Propagation :69%	
18.	IMPEDANCE :100±15%OHMS	
19.	Worst Case cable skew :45ns/100m	
20.	PoE compliance: Meets IEEE 802.3af and IEEE 802.3at for PoE applications	
21.	Warranty Three years comprehensive onsite warranty	
	Cat 6 UTP Loaded Patch Panel -	**Compliance (Yes/No)**
	Make & Model:	
1.	Patch Panel made of powder coated steel, in 24 port configurations Allow for a minimum of 200 re-terminations without signal degradation below standards compliance limit. Have port identification numbers on the front of the panel. Should have self-adhesive, clear label holders (transparent plastic window type) and white designation labels with the panel IDC: Suitable for 22-26 AWG stranded and solid	

	wire compatible with both 110 & Krone punch down tools Improved cable management with optional cable management bar Category 6 Unshielded Twisted Pair 4 pair should be complied as per ETL verification program for compliance with ANSI/TIA568.2-D standard	
2.	Plastic Housing: PBT+Glass Fiber, UL94V-0 rated	
3.	Operating Life: Minimum 750 insertion cycles Material: Phosher bronze with nickel plated Contact Plating: 50µ" Gold plated on plug contact area Contact Force: 20N max	
4.	Plastic Housing: Polycarbonate, UL94V-2 rated or equivalent IDC Contact Plating: Phosphor bronze with tin plated Wire Accommodation: 22-26 AWG solid Voltage Rating: 125V AC RMS Contact resistance: 20Milliohms Insulation resistance: 100 MegaOhms @ 500V DC	
5.	Three years comprehensive onsite warranty	
	Cat 6 UTP Patch cord	**Compliance (Yes/No)**
	Make & Model:	
1.	Category 6 Equipment cords – 1/2/3/5 Mtr The work area equipment cords shall, at a minimum comply with proposed ANSI/TIA/EIA-568-C.2 Commercial Building Cabling Standards Transmission Performance Specifications for 4 pair Category 6 Cabling. Equipped with modular 8- position modular plugs on both ends, wired straight through with standards compliant wiring.	
2.	Conductor size: 24 -26 AWG stranded bare copper Jacket: Low Smoke	
3.	Operating life: Minimum 750 insertion cycles Contact blade: Copper Alloy Contact plating: 03Mµ" Gold	
4.	Dielectric withstanding Voltage: 1000VDC or 700 VAC Insulation resistance: >500 MegaOhms @ 1000V DC/min Operating temperature: - 10oC to 60oC	
5.	Clear Polycoarbonate for RJ45 And Clear PVC for Boot	
6.	ISO/IEC 60603-7-4 and FCC 47 part 68	
7.	Factory molded Boot :Yes	
8.	Category 6 Unshielded Twisted Pair 4 pair should be complied as per ETL verification program for compliance with ANSI/TIA568.2-D standard	
9.	Three years comprehensive onsite warranty	
	Rack Specification - 19U / Width 600 / Depth 600	**Compliance (Yes/No)**
	Make & Model:	
1.	Conforms to DIN 41494 OR equivalent ISO Standards	
2.	Adjustable 19" equipment mounting verticals provide better mounting flexibility and maximizes the usable mounting space	
3.	Depth adjustable mounting slots	
4.	Precision engineering capabilities and best efficient software configuration product technology provide the best product quality and fastest delivery in the industry	
5.	Top and bottom Panel with ventilation and cable entry facility	
6.	Provision to mount cooling fans on the top panel	

7.	Powder coated finish with pretreatment process meeting all industry standards	
8.	Grounding and Bonding Options. 100% assured compatibility with all equipment conforming to DIN 41494 (General industrial standard for equipment)	
9.	Front Door : Lockable Toughened Glass Door	
10.	Mounting Angle : 19" Mounting angles made of formed steel	
11.	Top and Bottom Cover : Welded to Frame, Vented and Field Cable entry exit cut outs	
12.	Standard Accessories: Power Distribution Units, 1U Horizontal Cable Manager, FAN and one Hardware Packet	
13.	Warranty: Three years comprehensive onsite warranty	
	Rack Specification - 48U Closed Rack / Width 8000 / Depth 1000	**Compliance (Yes/No)**
	Make & Model:	
1.	Adjustable 19" equipment mounting verticals provide the better mounting flexibility maximizing the usable mounting space	
2.	Depth adjustable mounting slots	
3.	Precision engineering capabilities and best efficient software configuration product technology provides the best product quality and fastest delivery in the industry	
4.	Top and bottom Panel with ventilation and cable entry facility	
5.	Provision to mount the cooling fans on the top panel	
6.	Powder coated finish with pretreatment process meeting all industry standards	
7.	Grounding and Bonding Options	
8.	100% assured compatibility with all equipment conforming to DIN 41494. General industrial standard for equipment	
9.	Front Door : Lockable Toughened Glass Door	
10.	Equipment Mounting : DIN Standard 10mm Sq. Slots / Direct M6 Tap	
11.	Mounting Angle : 19" Mounting angles made of formed steel	
12.	Top and Bottom Cover : Welded to Frame, Vented and Field Cable entry exit cut outs	
13.	Mounting Option : Castor wheels (Front 2 wheels with Break and rear without break) Or Levelers Or Base plinth	
14.	Accessories: Doors & Side Panels, Power Distribution Units, Cable Manager, 4 * Fans and Fan Modules, Jacking Feet, 5 * Mounting Hardware, Vertical Power strip with 8 nos of 5/15A sockets (high end).	
15.	Warranty: Three years comprehensive onsite warranty	

Router Specifications

Sr.No.	Technical Specification for Router	Compliance (Yes/No)

	Make & Model:	
1.	Form Factor	
2.	19" Rack Mountable	
3.	Architecture	
4.	The router should be modular in architecture with single chassis solution	
5.	The router should have sufficient internal flash memory or more to support multiplesoftware images for backup purposes, log report and future scalability	
6.	The router should have sufficient RAM/DRAM or more to support large routing tables & other memoryintensive processes.	
7.	The router throughput of minimum 20 Gbps or more from day 1	
8.	The router should support Firewall	
9.	The router should have Redundant Power supply from day one	
10.	All modules / SFP, fan trays & Power supplies should be hot swappable	
11.	Interfaces	
12.	Minimum 4 x 1000Base-T and 4 x 1000Base-LX/LH (SM) SFP from day 1 (including required optics)	
13.	Should support 4 x 10G WAN Interfaces	
14.	Should IPv4, IPv6 routes and Multicast Routes	
15.	Protocols	
16.	Should support RIPv2, OSPF, IS-IS and BGPv4, BGPv4 Route Reflector, uRPF, LDP, BFD routing protocols & IP multicast routing protocols: IGMPv3, PIM SM, PIM SSM, RSVP, ERSPAN / port mirroring, IPSLA/ RPM, IKE, ACL/filters, DHCP, FRR, DNS, Segment Routing. Programmability Netconf/Yang /Restconf /RESTAPI, BGP-LS, NAT	
17.	Should support Enterprise Services feature set with support for protocols like Multiprotocol LabelSwitching (MPLS), MoFRR, Layer2 circuits, VPLS, VxLAN and EVPN	
18.	The router should support multiple level of privileges and authentication for user access	
19.	Should support RADIUS and TACACS+, Access List/ Firewall Filters, QoS, Policy based routing, IPv6, NTP, SNMP. Minimum 2000 ACLs, the router should support.	
20.	Should be capable of supporting 802.1q VLANs and VLAN trunking	
21.	Should support port aggregation for higher bandwidth and redundancy	
22.	Router should support minimum 16k hardware Queues	
23.	Router should support Hardware assisted CGNAT	
24.	The router should support congestion management techniques like Priority Scheduling, Router should support, QoS, CBWFQ/equivalent queuing	

	mechanism, Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR).	
25.	Router should support flow monitoring using NetFlow/sFlow/jflow/IPFIX	
26.	Security	
27.	The router should support stateful Firewall features, DES, 3DES,AES-128, AES-256, MD5, SHA, SHA 256, MACSec.	
28.	Router should support IPSEC tunnels.	
29.	The router should support out of band management	
30.	Should be possible to boot the router from a remote system or USB ports	
31.	Should support SNMP v1, v2 and v3	
32.	Should support TFTP for downloading of OS software	
33.	Should support online and extensive debugging features	
34.	Warranty & Support	
35.	3 year warranty support	
36.	All the licenses provided should be perpetual.	

Firewall Specifications

Sl.No	Item Description	Technical Specification	Compliance
1	**Make**	To be mentioned by the bidder/ Vendor	
2	**Model No.**	To be mentioned by the bidder/ Vendor	
3	**Country of Origin**	To be mentioned by the bidder/ Vendor	
4	**Hardware Architecture**	The proposed hardware based firewall should not consume more than 1RU Rack-mountable space	
		Proposed Firewall be multi-core CPU's based architecture to protect latest security threats.	
5	**Performance & Scalability**	Appliance must have one Console port, dedicated one management Port, two USB port and redundant power supply	
		The device should have 16 x 1G Copper ports 6 x 10G SFP+ ports from day 1.	
		Appliance should have 512 GB storage or more from day 1	
		Appliance should support 17 Gbps or more Firewall throughput & 9 Gbps or more IPS throughput.	
		Appliance should support 9.4 Gbps or more Threat Protection throughput	

		The device should have Concurrent Sessions: 4 Million or higher & New connection/Sec: 110,000 or higher	
		Firewall Should support at least 10 Gbps or more IPSec VPN throughput and 4000 IPSec Site-to-Site VPN tunnels & 1000 IPSec VPN clients.	
		Firewall Should support at least 5 Gbps or more TLS/SSL inspection & decryption throughput and 500 SSL VPN clients. The appliance should have 350,000 SSL DPI connections.	
6	**General Firewall Features**	Solution should provide unified threat policy like AV/AS, IPS, URL & Content filtering, Application control, Malware protection, Bandwidth management, policy & policy based routing on firewall rules to secure connectivity between Internet & internal network and security controls must be applied on inter zone traffic.	
		Should support BGP,OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2).	
		Firewall should support manual NAT and Auto-NAT, Static NAT, Dynamic PAT, PAT etc	
		Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode	
		Should support Zero-Touch registration & provisioning using mobile App.	
		solution should support policy based routing, Application based routing and also Multi Path routing.	
		Application Control : The proposed system shall have the ability to detect, log and take action against network traffic based on over 3500 application signatures	
		Should have extensive protocol support to identify common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decode payloads for malware inspection, even if they do not run on standard, well-known ports.	
		Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy.	
		Firewall should support static routing ,Dynamic Routing and WAN load-balancing for redundant or backup Internet connections.	
		The appliance should be capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports.	
		Should support deep packet SSL to decrypt HTTPS traffic for scanning (IPS, Gateway Antivirus, Content Filtering, Application control) transparently and send to destination if no threat found.	
		The Firewall should Support for TLS 1.3 to improve overall security on the firewall	
		Firewall should support clientless SSL VPN technology or an easy to manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms..	

		Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of	
		Solution should have inbuilt support of DES, 3DES, AES 128/192/256 encryption MD5, SHA and Pre-shared keys & Digital certificate based authentication connection tunnel.	
		Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.	
		Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Route-based VPN over OSPF, RIP, BGP.	
		Proposed solution must support application inspections on following protocols DNS,FTP,H.323 ,SMTP, SQLnet, RTSP, SMBv1/v2,SIP, NetBios, TFTP, SNMP etc.	
		Solution should support User identification and activity available through seamless AD/LDAP/Citrix/Terminal Services SSO integration combined with extensive information obtained through Deep Packet Inspection.	
		Should have secure SD-WAN that enables organizations to build, operate and manage secure, high-performance networks across remote sites for sharing data, applications and services using low-cost internet services without adding any additional components or hardware. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. Necessary licenses, if required, need to be provisioned from day 1.	
		Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP.	
		Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled..	
7	**Firewall Security Features**	Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV.	
		The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbound threats	
		Antivirus should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, HTTP, FTP etc	
		Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams..	
		Solution should have single-pass DPI architecture simultaneously scans for malware, intrusions and application identification and ensuring that all threat information is correlated in a single architecture	

		Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. Should have at least 7500 IPS Signatures or 20K DPI signatures, 80 million Could AV signatures.	
		Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.	
		Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify. URL database should have at least 15-20 million sites and 55 + categories.	
		Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy.	
		Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network.	
		Firewall should support HTTP Request tempering protection, Directory traversal prevention, SQL injection Protection, Crosssite scripting Protection (XSS) & DNS security	
		Should provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol.	
		Solution should support both on premise and cloud based Multi-engine Sandboxing for preventing zero day threats.	
		The Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. The technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen. The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc.	
		Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments.	
		Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined.	
		Deep packet SSL should be available on the same platform & License for DPI SSL should be along with appliance.	

		The Firewall solution should have detection and prevention capabilities for C&C communications and data exfiltration.	
		Firewall Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address.	
8	**High-Availability Features**	The proposed solution should support Hardware redundancy and should have Active-Passive configuration with Stateful Sync from day 1.	
		The proposed solution should support active-passive / standby / active high availability. The proposed solution should have Active/Passive HA from Day 1.	
		The device should support stateful session failover to a standby appliance in the event of a hardware failure without any manual intervention.	
9	**Visibility and Monitoring**	Should provide real-time monitoring and visualization provides a graphical representation of top applications , top address, top users and intrusion by sessions for granular insight into traffic across the network.	
		The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services information & High availability status.	
		Solution should support granular network visibility of network topology along with host info.	
		Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats.	
10	**Management & Reporting Feature**	The management platform must be accessible via a web-based interface and without any additional client software	
		Firewall should support management via Cli, SSH ,GUI and support for SNMPv2/3..	
		The solution should store syslog in local storage or remote appliance. OEM can offer individual solution for logging and reporting based architecture to meet the requirements.	
		Firewall should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.	
		Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks in different formats such as PDF/TEXT/ CSV	
		The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address	
		Analytics platform support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem	
		The solution should support Cloud-based configuration backup.	

		The solution should support IPFIX or NetFlow protocols for real-time and historical monitoring and reporting	
		The solution should support Application Visualization and Intelligence - should show historic and real-time reports of what applications are being used, and by which users. Reports should be completely customizable using intuitive filtering and drill-down capabilities.	
		Logging and reporting solution should be supported. Should have Multi Tenant and Device Group level management	
		Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.	
		The solution shall have readymade templets to generate reports like complete reports or attack reports, bandwidth report etc.	
11	**Certification, Warranty, Installation, Testing and Commissioning**	The Firewall solution offered must be ICSA certified (Till Q3 2022) for Network Firewall, Anti-virus, IPv6/USGv6 Certification.	
		The Firewall OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 97% in Exploit Block rate in the last NSS Lab for NGFW report (2019).	
		Proposed Solution should support 24x7x365 telephone, email and web-based technical support.	
		OEM should have TAC and R&D center in INDIA.	
		Manufacturer's warranty should be mentioned minimum 05 (five) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , ATP,Patch & Firmware upgrade.	
		Bidder must carry out on site installation, testing and commissioning.	

Controller Specifications

Sr.No	Hardware based Wireless Controller	Compliance (Yes/No)
1.	Controller Hardware Specification	
2.	It shall support minimum 4 x 10/100/1000 Mbps RJ-45 ports, 4 x 100/1000 Mbps SFP combo ports and if need for future expansion capability upto 10G arises then the same would be done with or without additional hardware during warranty period by the bidder.	
3.	It shall support Console Port.	
4.	Should support atleast one USB 2.0 port	
5.	Should support LED indicators for LAN	
6.	Should be a Rack Mountable appliance.	
7.	Controller should support minimum 100 AP's from day 1, and should include all type of license for lifetime use of minimum 100 AP's from day 1.	

8.	Controller can be upgradable up to 256 APs management.	
9.	Should support up to 250 VLANs and Upto 50 configurable SSIDs stored on the Controller.	
10.	Locally stored MAC address table Should support minimum 16,000 entries.	
11.	Support for at least 2500 log records.	
12.	Controller should support at least 7500 users and support for at least 3000 concurrent captive portal authentication users.	
13.	Should support CAPWAP or equivalent	
14.	Controller should support local user database of at least 20,000.	
15.	Power input should be 100 to 240 VAC, 50/60 Hz, and internal power supply.	
16.	Operating temperature should be 0 degree Celsius to +40 degree Celsius.	
17.	Certification: CE, FCC, EN/IEC 60950-1, and RoHS	
18.	Protocols	
19.	IEEE 802.3u & IEEE 802.3ab ax	
20.	Auto Negotiation & Auto MDI/MDIX support and IEEE 802.3x Flow Control	
21.	IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11d and 802.11h ax	
22.	Support Pause Frame at Full-Duplex operation and backpressure at Half-Duplex operation.	
23.	IGMPv1/v2 & IGMP snooping	
24.	Wireless LAN Access Point Management	
25.	AP firmware management.	
26.	AP configuration management Centralized RF settings.	
27.	AP monitoring Classify managed, rogue, and authenticated failed AP.	
28.	Monitor associated clients on each management AP.	
29.	Monitor ad-hoc clients.	
30.	L3 Features	
31.	Support for IPv4 and IPv6 static routing.	
32.	IPv6 router advertisement support	
33.	L3 roaming (inter-subnet) should be supported for roaming of clients across different subnets.	
34.	The controller should be configurable to operate as DHCP Server/Client/Relay	

35.	RF Planning/Monitoring & Roaming	
36.	Controller should support RF monitoring enabling the detection of Rogue AP.	
37.	Controller should provide functionality for Real time display of the wireless network topology including output transmit power display of each AP and associated clients of each AP along with client IP address and MAC address.	
38.	Should support AP RF channel adjustment, AP transmit output power adjustment	
39.	Controller should have capability to configure an AP for dedicated RF monitoring only enabling enhanced detection of Rogue AP and interference.	
40.	Controller should have coverage hole detection feature .It should alert when AP are down or compromised RF environment is detected. It should also have self-healing - Automatic neighboring AP power increase to fill in for coverage losses	
41.	Controller should support AP load balancing.	
42.	Support for fast roaming .This includes seamless rapid mobility across VLAN and subnet.(L2 & L3)	
43.	Controller should support IEEE 802.11r	
44.	Quality of Service & VLAN	
45.	Support for CoS,ToS and DSCP along with CoS to DSCP mapping	
46.	It should support 802.1p Priority Queues with min. 8 no. of Queue	
47.	QoS policy should be configurable per VLAN or based on source/destination TCP, UDP, IP and MAC address.	
48.	Should support Per Queue Minimum Bandwidth Guarantee, Per-Port Bandwidth Control (Traffic Shaping), Per-Flow Bandwidth Control	
49.	Should Support IEEE 802.11k	
50.	Support for 802.1q, Voice VLAN,MAC Based Vlan,802.1v,GVRP and Q in Q	
51.	Should support WMM & Unscheduled Automatic Power Save Delivery (UAPSD)	
52.	Should support SSID to VLAN mapping	
53.	Should support Spectralink Voice Priority (SVP)	
54.	Security	
55.	should support static and dynamic WEP with RC4 cipher suite of 64/128/152 bits	
56.	WPA Personal/Enterprise	
57.	WPA2 Personal/Enterprise with AES-CCMP cipher suite of 128/256bits with support to WPA3	
58.	Controller should have a WIDS-Wirelss intrusion detection system	
59.	Support Anti -spoofing checking and Denial of Service (DoS) Protection.	
60.	Should support feature to Block an Ad-hoc client from WLAN access	

61.	Filtering of untrusted DHCP messages received by the controller.	
62.	Should support External database: RADIUS, LDAP, Windows Active Directory, POP3	
63.	Support for 802.1X EAP types- EAP-MD5, EAP-TLS, EAP-TTLS, EAP- FAST, PEAP-GTC, PEAP-TLS, PEAP-MS-CHAPv2	
64.	Should support Local database (Permanent/ temporary user database), External database	
65.	Should support Captive portal for both wired or wireless user authentication	
66.	Should support Captive Portal with Configurable Portal Page, including image files.	
67.	Support Rogue AP Detection.	
68.	The wireless controller must protect against rogue AP by sending De-authentication messages to the rogue AP. Thus preventing clients connecting to the Rogue AP.	
69.	Isolation of clients connected to an AP	
70.	Should support email alert to admin based on different level event (emergency, alert, error, warning, notification, information)	
71.	Management & User accounts	
72.	Management interface HTTP ,SNMP v1/v2/v3,telnet ,secure sheel (SSH) logging and reporting	
73.	Diagnostics: Managed access point ping, DNS lookup and Traceroute.	
74.	Maintenance : Save /Restore configuration ,restore to factory defaults ,admin password change ,firmware upgrade via web browser for the wireless controller and the managed access points	
75.	Should support real-time monitoring displaying Traffic overview, Discovered AP, Bandwidth usage, WLAN statistics, CPU utilization and Memory utilization,	
76.	Single and Batch generation option for temporary guest accounts.	
77.	Each temporary account should have option to be accompanied by time-limited or volume-limited Internet access privileges. With feature to monitor and modify limit of any temporary Guest account.	
78.	Note	
79.	Wi-Fi Controller should be supplied with the all necessary components like Power cord, Rack mount bracket, Installation Guide, etc. and necessary software image file to fulfil all above mention feature set from day 1.	
80.	Operating Temperature	
81.	0° to 40° Celsius	
82.	Warranty and Support	
83.	Five year hardware/software warranty with on-site advance replacement by OEM directly within 24 hours	
84.	The vendor shall provide software fixes and updates as part of the warranty	
85.	The special features that need additional licensing along with its cost has to specified	
86.	All the licenses quoted should be perpetual. All the features and signatures including WIPS available at the time of expiration of license should continue to	

	work. Renewal of licenses should be required only for new features and updates/releases announced by the OEM after the contract expires	

Network Management System

Sr.No.	Network Management System	Compliance (Yes/No)
1.	NMS should Compliance to IEC 62443-4-1 or similar cyber security standards, Support server client architecture and Support multi-tenant architecture, NMS Server will support 5000 Devices from day1 and can upgraded for 5000+ Devices if required. Supports both for Windows and Linux OS platform	
2.	Support High Availability (HA), this can be used to reduce the load on one server, while increasing the reliability of the system by being able to survive failures. NMS can be installed in a HA deployment type, providing fault tolerance and allowing individual nodes to be taken offline without impacting the network.	
3.	Support probe design to collect data from remote site without VPN or behind NAT	
4.	Compliance to FCAPS or similar network management framework and Should support sFlow based traffic monitoring.	
5.	Should support role-based user management with Radius authentication, Should support traditional network topology and VLAN based topology and Should support device panel simulation and visualization of device rack	
6.	Should support IPv4 and IPv6 based devices discovery and built-in MIB Browser and MIB Complier	
7.	Support SNMP v1, v2c, v3 scan, support smart scan by neighborhood and Support discover across LAN by probe	
8.	Support periodically discovery with specific time period and Support LLDP, FDB based link discovery	
9.	Support overall system and product summary and Support customized dashboard, NMS allows for the creation of customized dashboards that contain a variety of different metrics. Separate dashboards between different users, the users must be in different workspaces. NMS allow to show device details overview gives a more complete dashboard view of a device. The default overview tab displays basic information that allows network administrators to get the information they need as quickly as possible	
10.	Support auto-topology generation, support customized topology generation, Support devices status display, Support link status display, Support different structure of topology (tree type, start type), Support multi-layer topology for following views, Support customized background image overlay for following views	
11.	Support multiple polling methods - Ping and SNMP and Support customized polling time for each devices or by group	
12.	Support customized criteria or threshold to trigger the event based on following rules - Value Match, Keyword Match, Keyword Combination Match and Support customized escalation rules and Support email notification to defined users	
13.	NMS should support periodically scheduled config backup for single or multiple devices	
14.	NMS should support config restore by system-stored or user by user uploaded file for single or multiple devices	
15.	The User / Workspace view shows all of the user accounts and all of the available work spaces.	
16.	Users on the NMS server can be assigned to a specific workspace, which can be configured to limit the amount of or type of devices that are available to those users	
17.	The report feature is used to generate reports that will help you monitor system and network health as well as troubleshoot problems. Reports can be generated to run	

	on an immediate one-time use or a scheduled basis, and can be customized by certain user-defined criteria.	
18.	Generated reports can be formatted into graphs or tables and be downloaded for future use as PDFs	
19.	NMS should provide reports monitoring for various statistical information by device and ports.	
20.	The System Logs view shows a list of all events that have taken place on the NMS server. Events may be filtered by entering a keyword into the search box.	
21.	Wired Traffic Reports page is used to issue reports monitoring wired traffic by port and by device	
22.	Report should displays the following minimum information: Number, Recurrent status, Name, Status, Time of Creation, Number of Targeted Devices, Creator, and Next Execution Time.	
23.	Support to NMS administrator to manage the SNMP traps on the system. New traps can be added, traps can be deleted, and a description can be given to the traps, so that they can be more easily identified.	
24.	NMS should support Configuration Comparison with two different configuration files and highlight the differences.	
25.	You can select files from either all devices or from a specific device and following actions: Reload Configuration File, Save As, Restore to Device Between the two panels, you are able to toggle locked scrolling and copy highlighted chunks of text between the two configuration files	
26.	Firmware Management is used to deploy firmware upgrades to multiple devices at the same time. Firmware Management view is used to manage the deployment and tracking of firmware to devices on the network. File Management is used to manage uploaded firmware and configuration files. The File management page allows you to manage uploaded firmware and configuration files	
27.	Configuration Management is used to backup and restore configurations for a single or multiple devices at the same time. Configuration Management view is used to backup and restore configurations for a single or multiple devices at the same time.	
28.	NMS should support Task Management for use to view and manage currently running as well as historical task.	
29.	Batch Configuration contains a number of different pre-defined templates that can be used to configure multiple devices at the same time. It is also possible to use the built-in Script Template editor to create customized templates that can be saved for later use. NMS should support script dispatch with variables (such as IP, system name, etc.) defined by each device.	
30.	NMS should support various views that give network administrators a visual overview of different aspects of their network. The Device View list all of the discovered devices by category. Topology view shows how devices are interconnected with the use of topology maps. Rack View can be used to simulate physical racks, and network stack layouts. Event View keeps a log of all received events by discovered devices in chronological order. Monitor Logs displays captured Trap and Syslog messages from devices on the network. Support panel and LED status of switches and Support panel view with stacking switches	
31.	Devices that have support for local or remote logging will have a logs tab, which lists all of the events for that device. NMS supports both the Trap and Syslog standards and can receive either if a remote networking device is configured properly. The Logs view can be filtered by time period using the drop down menu. The events are listed in chronological order, starting with the name of the event, the SNMP version that was used	
32.	NMS support configuration of Every class of device can create its own default sensors that can be accessed from the device detail sensors tab. For example, Switches will have sensors for different types of metrics that relate to wireless clients, wireless traffic, or ping time. While routers and switches will have sensors that show metrics such as CPU utilization, wire speeds, and wired error packets.	

33.	The Sensor Settings view shows a list of available sensors based on the type of data collected by the sensor. The sensors configured here will show up as a widget on the dashboard of a device that the sensor is assigned to. Certain sensors will not be applicable to specific types of devices (e.g. Wireless sensors for switches or other devices that have no wireless capability). To create a new sensor for a single device or multiple devices, select the sensor type based on the desired data to be collected, and click on the New Sensor button.	
34.	Support inventory and devices export and Support devices grouping by label, a device can belong to multiple label, Inventory list shows hardware devices that are on the network and their relevant information such as IP address, Serial Numbers, and Firmware	
35.	The Notification Center shows the notification rules that have been configured for devices in NMS. The name of the notification rule is entered, and then the sensor type, device and alert conditions are selected. These are the conditions that will trigger the alert	
36.	Warranty : Three years comprehensive onsite warranty	

Note: The Passive Components Should be ETL Verified/UL listed and all copper components should be available on OEM website.

Certificates are mandatory.

Annexure-V- TECHNICAL BID COMPLIANCE INFORMATION – Bill of Quantity

Note: Bidders to ensure that the detailed technical specifications mentioned on Annexure III and IV in this tender are complied

Sr. No.	Item	Qty.	Unit
1.	Dual Band WiFi 6 Access Points	80	nos.
2.	Wireless LAN controller	1	nos.
3.	24 Port PoE Access Switch	2	nos.
4.	24 Port Aggregation PoE Switch	11	nos.
5.	24 Port Core Switch	1	nos.
6.	24 Port Access Switch	28	nos.
7.	Core Router	1	nos.
8.	SFP modules, SM, 1Gbps	4	nos.
9.	SFP modules, SM, 10Gbps	24	nos.
10.	CAT 6 Cable	17	box
11.	24 port Patch Panel	40	nos.
12.	CAT 6 Patch cord 1m	150	nos.
13.	CAT 6 Patch cord 2m	50	nos.
14.	IO CAT 6, 1 Port	100	nos.
15.	Fiber Optic 12F Cable	2000	m
16.	Fiber Optic Patch cord SM, LC-LC, 3m	100	nos.
17.	Fiber Optic Pigtail SM, SC, 3m	100	nos.
18.	LIU 12F, 19” Rack Mountable, with couplers and accessories	14	nos.
19.	LIU 24F, 19” Rack Mountable, with couplers and accessories	1	nos.
20.	LIU 48F, Wall Mount, with couplers and accessories	1	nos.
21.	19” 12U Rack	14	nos.
22.	Termination of CAT 6 cable in IO Box	100	nos.
23.	Termination of CAT 6 Cable on Patch Panel	100	nos.
24.	PVC Conduit ISI Mark, 32mm / 40mm	3200	m
25.	In Building laying of UTP CAT 6e	3200	m

26.	Fiber Optic Cable Termination	60	nos.
27.	HDPE PLB Pipe, 32/26 mm	200	m
28.	HDPE PLB Installation (Outdoor – Underground 1m, Soft Soil)	150	m
29.	HDPE PLB Installation (Outdoor – Underground 1m, Concrete)	50	m
30.	Project Management, Installation, Commissioning & Testing	1	nos.
31.	UTM firewall	1	Nos.
32.	NMS	1	Nos.

Note: 25Yr. Performance after successful installation (For cabling system)

Annexure-VI- (Authorization to be taken from Hardware OEM)

Ref. No. _____ Date:_____

To

The Managing Director,
H.P. State Electronics Development Corporation Ltd.,
First Floor, IT Bhawan, Mehli, Shimla-171013.

Subject: Tender reference No. HPSEDC/WiFi-HighCourt/2K23-5026

Sir,

Please refer to your request for proposal for Supply, Installation & Commissioning of Firewall & Wifi Network Accessories in High Court of H.P.

M/S _____ (Bidder), who is our reliable distributor/partner for the last _____years, is hereby authorized to quote on our behalf for the subject mentioned tender.

M/S _____ (Bidder) is likely to continue as our business partner during years to come.

We undertake the following regarding the supply and installation of Hardware for Supply, Installation & Commissioning of Firewall & Wifi Network Accessories in High Court Premises as described in the said tender:

We confirm that the product(s) quoted are not "end of life or end of sale products" as on Bid Submission date. If in case the support for the product quoted has been stopped/ withdrawn till the time of delivery of equipment, the same will be changed with the equivalent or superior product at no extra cost.

We also undertake that the support including spares, patches, and upgrades for the quoted products shall be available for 5 years from the signing of contract.

Yours faithfully,

(NAME) (Name of Manufacturer)

Note: This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having Authorization Letter to bind the manufacturer. It should be included by the Bidder in its bid.

ANNEXURE VII – FINANCIAL BID

Sr. No.	Item	Unit Basic Price	Qty.	Unit	Amount
1	Dual Band WiFi 6 Access Points		80	nos.	
2	Wireless LAN controller		1	nos.	
3	24 Port PoE Access Switch		2	nos.	
4	24 Port Aggregation PoE Switch		11	nos.	
5	24 Port Core Switch		1	nos.	
6	24 Port Access Switch		28	nos.	
7	Core Router		1	nos.	
8	SFP modules, SM, 1Gbps		4	nos.	
9	SFP modules, SM, 10Gbps		24	nos.	
10	CAT 6e Cable		17	box	
11	24 port Patch Panel		40	nos.	
12	CAT 6e Patch cord 1m		150	nos.	
13	CAT 6e Patch cord 2m		50	nos.	
14	IO CAT 6, 1 Port		100	nos.	
15	Fiber Optic 12F Cable		2000	m	
16	Fiber Optic Patch cord SM, LC-LC, 3m		100	nos.	
17	Fiber Optic Pigtail SM, SC, 3m		100	nos.	
18	LIU 12F, 19” Rack Mountable, with couplers and accessories		14	nos.	
19	LIU 24F, 19” Rack Mountable, with couplers and accessories		1	nos.	
20	LIU 48F, Wall Mount, with couplers and accessories		1	nos.	
21	19” 12U Rack		14	nos.	
22	Termination of CAT 6 cable in IO Box		100	nos.	
23	Termination of CAT 6 Cable on Patch Panel		100	nos.	
24	PVC Conduit ISI Mark, 32mm / 40mm		3200	m	
25	In Building laying of UTP CAT 6e		3200	m	
26	Fiber Optic Cable Termination		60	nos.	
27	HDPE PLB Pipe, 32/26 mm		200	m	

28	HDPE PLB Installation (Outdoor – Underground 1m, Soft Soil)		150	m	
29	HDPE PLB Installation (Outdoor – Underground 1m, Concrete)		50	m	
30	Project Management, Installation, Commissioning & Testing		1	nos.	
31	UTM firewall		1	Nos.	
32	NMS		1	Nos.	
33	Dual Band WiFi 6 Access Points		80	nos.	
34	Wireless LAN controller		1	nos.	
	Total				
	GST @ 18%				
	Total Cost with Tax				