



**NOTICE INVITING TENDER FOR
TRUNKY BASIS**

**PROCUREMENT OF INSTALLATION AND COMMISSIONING OF CAMPUS NETWORK
INFRASTRUCTURE AT DMRL AND ATC CAMPUS**

Ref: ITI/2026-27/Def/Mktg/CNI

ITI LIMITED

**(A Govt. of India Enterprise)
Defence-Marketing
ITI Limited, First Floor, Core 6,
Scope Complex, Lodi Road, New Delhi-110003
website: <https://www.ityltd.in/>
Email: skumar_bcdel@ityltd.co.in
CIN No: L32202KA1950GOI000640**

1. Introduction.

ITI Limited, a Public Sector Undertaking under the Department of Telecommunications, Ministry of Communications, is a leading Telecom equipment manufacturer and solution provider in India. The major customers are BSNL, BBNL, MTNL, Defense, Paramilitary forces, Railways, Banks, Central & State Govt. departments, Institutions and research organizations like ISRO.

ITI Limited has been undertaking various projects in all fields of telecommunications and information technology and also continuously deploying new technologies in the field of Telecom, ICT, Networking, e-Governance etc. ITI has diversified its operation and has been executing projects in the field of Smart Infrastructure (Smart Cities, Safe Cities, Smart Energy Meters, Smart Classrooms, Smart Poles etc), Bharatnet etc. ITI has been executing projects in latest technologies like GPON, OLT, ONT, OFC, HDPE etc.

ITI Limited would like to address the tender on turnkey basis for selection of backend partner for procurement of for procurement of a Procurement of Installation and commissioning of campus network infrastructure at DMRL and ATC campus for DRDO. In this connection ITI Limited, invites sealed tender from eligible bidders for addressing the above tender opportunity and implementing the project as per their scope of work finalized with ITI.

2. Important Dates.

Date of tender Upload	17-09-2026
Due Date for tender Submission	08-10-2026 up to 03:00 PM
Estimated Cost (Approx.)	Rs. 29,86,47,550/-
Technical Specification	As per mentioned in GeM Bid- GEM/2026/B/7934036 Dated: 02-09-2026
Pre Empanelment Queries/Pre Bid meeting	NO
ITI Contact Person	Mr.Sandeep Kumar, DGM-Projects Ph.:011-24368533,24360555 Email:-skumar_bcdel@itilttd.co.in https://www.itilttd.in Helpdesk: Mr.Faiz Ahmad Khan, AM-Projects e-mail: faizahmad_nsu@itilttd.co.in
Tender Fee	Rs. 5,000/-+ Rs. 900/- = Rs. 5,900/-(Non-Refundable)
Earnest Money Deposit (EMD)	Rs. 5972951/-
PBG/Security Deposit/e-PBG	5%
Duration of e-PBG required (Months)	50
All other additional terms and Condition	As mentioned in Bid document.
The Bank Details of ITI Limited for NEFT/RTGS/Net Banking :	The Bank Details of ITI Limited for NEFT/RTGS/Net Banking is as below:

	Online RTGS/ NEFT Bank: State Bank Of India, Industrial Finance Branch, Residency Road, Bangalore-560025 MICR: 560002059 IFSC: SBIN0009077 A/C No.: 10637729843 EMD may also accepted in the form of BG
Mode of submission	Thru ITI e-tender portal https://itilimited.ewizard.in/ .

3. Tender Scope of work & Technical compliance:-

As per Tender Reference/Bid Number: GEM/2026/B/7934036 Dated: 02-09-2026 ITI inviting TENDER/BID for selection of backend partner for Procurement of Installation and commissioning of campus network infrastructure at DMRL and ATC campus for DRDO. The scope of this project as mentioned in Appendix-B. All the technical specification must compliance as per customer bid.

4. Instruction to Bidders

The bidders are required to submit soft copies of their bid electronically on the e-Wizard Portal using valid Digital Signature Certificates. Below mentioned instructions are meant to guide the bidders for registration on the e-Wizard Portal, prepare their bids in accordance with the requirements and submit their bids online on the e-Wizard Portal. For more information, bidders may visit the Portal (<https://itilimited.ewizard.in/>).

a. REGISTRATION PROCESS ON ONLINE PORTAL:

Bidders to enroll on the e-Procurement module of the portal <https://itilimited.ewizard.in/> by clicking on the link “Bidder Enrolment”.

- The bidders to choose a unique username and assign a password for their accounts. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. This would be used for any communication from the e-Wizard Portal.
- Bidders to register upon enrolment, with their valid Digital Signature Certificate (Class III Certificates with signing and Encryption key) issued by any Certifying Authority recognized by CCA India with their profile.
- Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSCs to others which may lead to misuse.
- Bidder then logs in to the site through the secured log-in by entering their user ID/password and the password of the DSC / e-Token.
- After registration send mail to Helpdesk: helpdeskeuniwizarde@gmail.com for Account activation.
- As per portal norms Registration Fee will be applicable.

b. TENDER DOCUMENTS SEARCH:

- Various built-in options are available in the e-Wizard Portal like Department name, Tender category, estimated value, Date, other keywords, etc. to search for a tender published on the Online Portal.
- Once the bidders have selected the tenders they are interested in, they may download the required documents/tender schedules. These tenders can be moved to the respective ‘Interested tenders’ folder.

- c) The bidder should make a note of the unique Tender No assigned to each tender, in case they want to obtain any clarification/help from the Helpdesk.

5. BID PREPARATION:

- a) Bidder should take into account any corrigendum published on the tender document before submitting their bids.
- b) Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.
- c) Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that needs to be submitted. Any deviations from these may lead to rejection of the bid.
- d) Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document/schedule and generally, they can be in PDF/XLSX/PNG, etc. formats.

5(i)	Eligibility Criteria of Applicants	
	a	<u>Company Profile:</u> The Bidder shall be a Company incorporated /registered in India under Companies Act 1956/2013/ proprietorship/ partnership firm/ Limited Liability Partnership (LLP) and should be in operations continuously for at least 5 years as on the last date of submission of bid. 1) In case the bidder has executed any work/project with/for ITI in the last 5years, it is essential that a satisfactory certificate signed by at least DGM level/or above officer from ITI to be submitted for such project. 2) In case CMC followed by project execution, the CMC charges quoted by bidder are optional and ITI reserves the right to either award CMC to the bidder or float a separate tender at the end of project completion which will be abide by bidder. 3) Any financial liability (like contract processing fee, Agreement Stamp fee, Portal fee, BG making fee etc.) on ITI for this project will be borne by Bidder.
	b	a) Minimum average Turnover during each of the last three financial years (FY 2022-23, 2023-24 & 2024-25).should be at least 895 Lakh (s) b) Net Worth of the bidding entity during each of the last three financial years (FY 2022-23, 2023-24 & 2024-25) should be in positive. c) The Bidder shall submit copy of Audited statements/CA certificate for last three years should be submitted along with technical proposal.
	c	Procurement of Installation and commissioning of campus network infrastructure at DMRL and ATC campus for DRDO. For more details refer to scope of work as per GeM BID Documents.
	d	The bidder should not have been blacklisted or debarred by any Pvt Ltd/State / Central Government or their agencies or Public Sector Undertakings (PSUs) as on bid submission date for corrupt, fraudulent or any other unethical business practices or for any other reason. Undertaking as per the format attached in Annexure-I duly signed by authorized signatory of bidder.
	e	All the applicable annexures and documents is as per customer BID.
	f	The supply item/OEM must be as per manufacturer certifications mentioned in BID. The technical specification of all the supplied items/ equipments as per the Operational characteristics and features as mentioned in bid Appendix-B. All the above sites/solution & technical specifications must be complied with the original GeM Tender.
	g	Undertaking for willingness to work with ITI as per customer tender etc. terms and conditions.

	h	EMD (Back to Back Basis): The bidder seeking EMD exemption, must submit the valid supporting document for the relevant category as per GeM GTC with the bid. Under MSE category, only manufacturers for goods and Service Providers for Services are eligible for exemption from EMD. EMD & Performance security should be in favour of Beneficiary, wherever it is applicable. EMD of unsuccessful bidders should be returned back once the contract is finalized. The bidder seeking EMD exemption, must submit the valid supporting document for the relevant category as per GeM GTC with the bid. EMD & Performance security should be in favour of Beneficiary, wherever it is applicable.
	i	Undertaking expressing willingness to sign agreement with ITI.
	j	Bidder shall provide valid OEM Authorization Certificate for all the products quoted as well as certify that the proposed product is not declared end of sale. OEM documents and all applicable annexures/appendix shall be provided as per required by customer RFP
	k	Consortium is not allowed. Bid splitting not applied. No part bidding allowed.
	l	ITI reserve the right to reject /cancel the bid at any time without assigning any reason.
	m	The agency should have successfully completed similar works(definition of similar Work should be clearly defined) during the last five Years ending last day of the month Previous to the one in Which bids are received as indicated below: i. Three similar completed works each costing not less than 20% Of the estimated cost of work. OR ii. Two similar completed works each costing not less than 25% of the estimated cost of work OR iii. One similar completed work costing not less than 40% of the estimated cost of work. . Similar Work:-The bidder/OEM must have the experience in the same field as mention in work scope and technical specification.
	n	Our company reserves the right that if any product, service or equipment is being manufactured in ITI limited , its supply and service must be provided to us by the vendor.
	o	Warranty:- Warranty period of the supplied products shall be 3 years from the date of final acceptance of goods or after completion of installation, commissioning & testing of goods (if included in the scope of supply), at consignee location. OEM Warranty certificates must be submitted by Successful Bidder at the time of delivery of Goods. The seller should guarantee the rectification of goods in case of any break down during the guarantee period. Seller should have well established Installation, Commissioning, Training, Troubleshooting and Maintenance Service group in INDIA for attending the after sales service. Details of Service Centres near consignee destinations are to be uploaded along with the bid.
	p	Generic:- Bidders shall quote only those products (Part of Service delivery) in the bid which are not obsolete in the market and has at least 7 years residual market life i.e. the offered product shall not be declared end-oflife by the OEM before this period.
	q	Average Annual Turnover:- Minimum average annual turnover for last three financial years, ending 31st March of the previous financial year,should not be less than 30% of estimated cost of the Buy (Indian-IDDM) and Buy (Indian) project and for Buy & Make (Indian) should not be less than 30% of estimated cost of the Make portion.
5(ii)		General : Provide Compliance for the following
		YES/NO

	a	All activities like Proof of concept on “No Cost No Commitment” (NCNC) basis wherever applicable will be the responsibility of bidders	
	b	Bidder should be willing to impart required training during undertaking services & execution of project (if applicable)	
	c	Bidder should be willing to sign an exclusive agreement with ITI for smooth execution of the project and all commercial terms will be as per the customer Tender/PO on back-to-back basis.	
	d	PBG will be taken from back-end partner, once ITI will be declared L1. Performance Bank Guarantee (PBG) required for the bid will be borne by the selected bidder.	
	e	LD Clause: LD shall be as per ITI Clauses (@ 0.5% of order value per week or part thereof subject to a maximum of 10% of the undelivered portion/ the order value (if the item(s) cannot be used unless full supply is made) or to cancel the order and purchase the materials from alternative source at the risk and cost of the supplier) OR as per the customer PO/tender clause whichever is higher.	
	f	Payment Terms: a) Payment terms will be as per back to back basis. b) Payment to the vendor shall be done after deduction of all i. LD/recoveries imposed by customer (if any) ii. ITI's margin	
	g	The bidder shall give an undertaking for the following: a. To extend end to end support of partnership b. To support ITI and bid in this tender with ITI as lead bidder c. To support ITI for preparation of the tender, post bid clarifications, technical presentations and any other requirements as per tender.	
	h	Delivery Schedule: Delivery Schedule as per the customer Bid/Tender/ PO on back-to-back basis.(if applicable)	
	i	Consignee Details: As per bid and if any changes will be provided after the award of the work	
	j	Bidder will be responsible for any shortcoming in the BOM and the same should be rectified free of cost	
	k	Bidder should not be insolvent (Self Declaration).	
	l	ITI reserve the right to reject or cancel the bid at any time without assigning any reason.	
5(iii)		Checklist of documents/information to be submitted: (These documents shall be used for evaluating technical parameters for bidder qualification.)	
	a	Company Profile	
	b	Certificate of Incorporation a per clause 5(i)(a)	
	c	Memorandum & Articles of Association	

	d	Audited financial statements for the last 3 years (FY 2022-23, 2023-24 & 2024-25)
	e	GST Registration Certificate
	f	Copy of PAN Card
	g	CIN (Corporate Identity Number), if applicable
	h	Any other relevant registration documents on registration with other appropriate authorities (ESI, EPFO, etc.)
	i	Authorization letter in the company letterhead authorizing the person signing the bid for this tender and Power of Attorney (POA).
	j	Undertaking in letter head to indemnify ITI from any claims / penalties / statutory charges, liquidated damages, with legal expenses etc.
	k	Undertakings in Company letter head as per Annexure I.
	l	Bidders Details as per Annexure II.
	m	Clause by clause compliance of tender terms with references to supporting documents as per Annexure III.
	n	Pre-Contract Integrity Pact as per Annexure-V a) "Bidders participating in the tender have to agree to sign Integrity Pact on placement of order / contract" b) "Those bidders who are not willing to sign Integrity Pact will not be considered for bid opening"
	o	The bidder should give an undertaking on the company's letterhead that all the documents/certificates/information submitted by them against this tender are genuine.
	p	Bidder shall submit technical data sheet by highlighting each complied specification. Wherever technical specifications and operational/functional requirements not mentioned in datasheet, OEM compliance shall be submitted.
	q	Work order / Contract clearly highlighting the scope of work, Bill of Material and value of the contract/order; and Completion / Commission Certificate issued & signed by the competent authority of the client entity on the entity's Letterhead.
	r	Complete tender and customer tender document duly signed and stamped on each page by the bidder be uploaded.
	s	Conditional bids will not be entertained and summarily rejected. Only online bids on https://itilimited.euniwizarde.in portal will be accepted and no physical bids will be accepted.
5(iv)		Financial Bid:
		L1 Evaluation Method: A- Lump sum Quote for supply and service items as per Schedule of Requirements (SoR) and Scope of Work (SoW) in INR (without Taxes) B- Margin to ITI as a percentage of A C - Absolute value of Margin = A*B D- Overall Quoted price=A-C • During evaluation bidders with least "D" will be considered as L1. • The bid having higher value of "B" will be selected in case of tied D.

		If the bidder is selected, during the final tender submission, the price to be quoted shall not be more than price “A” and the margin offered to ITI shall not be less than “B” SoR & SoW Was as per Tender document and all clarifications & Amendments/Corrigendum
--	--	---

6. BID SUBMISSION:

- Bidder to log into the site well in advance for bid submission so that he/she uploads the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
- The bidder to digitally sign and upload the required bid documents one by one as indicated in the tender document.
- Bidders to note that they should necessarily submit their financial bids in the prescribed format given by department and no other format is acceptable.
- The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, the opening of bids, etc. The bidders should follow this time during bid submission.
- All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data, which cannot be viewed by unauthorized persons until the time of bid opening.
- The uploaded tender documents become readable only after the tender opening by the authorized bid openers.
- Upon the successful and timely submission of bids, the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.
- The off-line tender shall not be accepted and no request in this regard will be entertained whatsoever.
- As per portal norms Tender Processing Fee will be applicable.

7. AMENDMENT OF BID DOCUMENT:

At any time prior to the deadline for submission of proposals, the department reserve the right to add/modify/delete any portion of this document by the issuance of a Corrigendum, which would be published on the website and will also be made available to the all the Bidder who has been issued the tender document. The Corrigendum shall be binding on all bidders and will form part of the bid documents.

8. ASSISTANCE TO BIDDERS:

- Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.
- Any queries relating to the process of online bid submission or queries relating to e- Wizard Portal, in general, may be directed to the 24x7 e-Wizard Helpdesk. The contact number for the helpdesk is 8448288994/86/87/89/88/81/90/92/82 011-49606060, 07903269552, 9355030608, 9055030613, 7903810198, 9355030606, 9315620706, 9355030623, 9355030628, 8800526452, 9205898228, 9122643040, 9355030604, eprochelpdesk.01@gmail.com, eprochelpdesk.44@gmail.com, eprochelpdesk.06@gmail.com.
- The tender inviting authority has the right to cancel this e-tender or extend the due date of receipt of the bid(s).
- The bid should be submitted through e-Wizard portal (<https://itilimited.ewizard.in/>) only.
- All payments should be done through e-Wizard Payment gateway.

09. Special Conditions of tender:

- No advance will be paid to the bidder, even though ITI is eligible to get advance from the customer being a front end bidder.
- The selected bidder, who has partnered with ITI for a particular tender/ project shall not partner with any other lead bidder for the same tender/project

- c. If the bidder is selected, during the final tender submission, the margin offered to ITI shall not be less than the quoted price.

10. Special Conditions of TENDER:

- a. No advance will be paid to the bidder, even though ITI is eligible to get advance from the customer being a front end bidder.
- b. The selected bidder, who has partnered with ITI for a particular tender/ project shall not partner with any other lead bidder for the same tender/project
- c. If the bidder is selected, during the final tender submission, the margin offered to ITI shall not be less than the quoted price.
- d. The estimated project amount stated in this document is provisional and subject to revision during the actual bidding process. Consequently, the bidder's quoted amount may also fluctuate (increase or decrease).
- e. The work order for the actual RFP will be awarded based on the ratio of the bidder's quoted amount to the revised estimated project value, as compared to the initial estimated value stated in this document."
- f. The requisite final solution to all the supplied equipments/Services must be end to end support till final solution as per RFP clause.

11. Other Terms and conditions:

Confidentiality

- a) All documents, drawings, samples, data, associated correspondence or other information furnished by or on behalf of the Procuring Entity to the contractor, in connection with the contract, whether such information has been furnished before, during or following completion or termination of the contract are confidential.
- b) If advised by the Procuring Entity, all copies of such information in original shall be returned on completion of the contractor's performance and obligations under this contract.

12. Transparency

All procuring authorities are responsible and accountable to ensure transparency, fairness, equality, competition and appeal rights. This involves simultaneous, symmetric and unrestricted dissemination of information to all likely bidders, sufficient for them to know and understand the availability of bidding opportunities and actual means, processes and time limits prescribed for completion of registration of bidders, bidding, evaluation, grievance redressal, award and management of contracts.

It implies that such officers must ensure that there is consistency, predictability, clarity, openness, equal opportunities in processes.

13. Fall Clause:

Fall clause is a price safety mechanism in rate contracts. The fall clause provides that if the rate contract holder reduces its price or sells or even offers to sell the rate contracted goods or services following conditions of sale similar to those of the rate contract, at a price lower than the rate contract price, to any person or organization during the currency of the rate contract, the rate contract price will be automatically reduced with effect from that date for all the subsequent supplies under the rate contract and the rate contract amended accordingly.

The provisions of fall clause will however not apply to the following:

- i. Export/Deemed Export by the supplier;
- ii. Sale of goods or services as original equipment prices lower than the price charged for normal replacement;

- iii. Sale of goods such as drugs, which have expiry date;
- iv. Sale of goods or services at lower price on or after the date of completion of sale/placement of order of goods or services by the authority concerned, under the existing or previous Rate Contracts as also under any previous contracts entered into with the Central or State Government Departments including new undertakings (excluding joint sector companies and or private parties) and bodies.

14. Price Variation

A suitable price variation formula should also be provided in the tender documents, to calculate the price variation between the base level and scheduled delivery date.

15. Risk Purchase

If the empanelled partner fails to adhere to the quality norms, delivery schedules and other terms and conditions contained in this Tender after acceptance of purchase order and if no agreement is reached on the revised delivery schedule maximum up to 15 Business Days, then buyer shall have the liberty to procure the material from an alternate source at the Empanelled partner's risk and cost, and the Empanelled partner shall be liable to make good the loss incurred by Buyer in this process.

16. Indemnity:

The empanelled partner to indemnify ITI from any claims / penalties / statutory charges, liquidated damages, with legal expenses etc as charged by the customer. LD/ Penalties incurred on account of delay in supply, product failure during warranty if any and deficiency in Warranty and AMC services attributable to the partner shall be borne by the partner All terms and conditions of the customer tender/PO will be applicable to the empanelled partner on back to back basis without affecting the margin of ITI.

17. Arbitration:

Any dispute arising out of this TENDER shall be settled and resolved by any such Authorized person appointed by Chairman and Managing Director of ITI Limited.

18. Set Off:

Any Sum of money due and payable to the supplier under this contract may be appropriated by the purchaser or any other person contracting through the ITI and set off the same against any claim of the purchaser for payment of a sum of money arising out of this contract or under any other contract made by the supplier with the purchaser.

19. The interested partner may like to discuss the customer tender related information, TENDER Bidding Conditions, Bidding Process and clarifications, if any with the Deputy General Manager-Marketing

20. Intellectual Property Rights:

- i. All deliverable, outputs, plans, drawings, specifications, designs, reports and other documents and software submitted by the contractor under this contract shall become and remain the property of the procuring entity and subject to laws of copyright and must not be shared with third parties or reproduced, whether in whole or part, without: the procuring entity's prior written consent.
- ii. The contractor shall, not later than upon termination or expiration of this contract, deliver all such documents and software to the procuring entity, together with a detailed inventory thereof.
- iii. The contractor may retain a copy of such documents and software but shall not use it for any commercial purpose.

21. Language of offers:

The offers prepared by the Company and all the correspondences and documents relating to the offers exchanged by the companies shall be written in English language.

22. In the event that ITI is required to provide demonstration or working of the product to their buyers, the same shall be arranged by the bidder selected partner/OEM at latter's cost and expenditure.

23. Cost of TENDER:

The bidder shall bear all costs associated with the preparation and submission of his offer against this TENDER, including cost of presentation for the purposes of clarification of the offer, if so desired by ITI. ITI will, in no case be responsible or liable for those costs, regardless of the conduct or outcome of the TENDER process.

24. Purchaser's Right to accept any bid and to reject any or All Bids or to cancel the TENDER:

ITI Limited reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids, at any time prior to award of contract without assigning any reason whatsoever and without thereby incurring any liability to the affected bidder or bidders on the grounds of purchaser's action.

25. Amendment of TENDER:

At any time prior to the last date for receipt of offers, ITI, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the TENDER document by an amendment. In order to provide prospective bidder reasonable time in which to take the amendment into account in preparing their offers, ITI may, at their discretion, extend the last date for the receipt of offers and/or make other changes in the requirements set out in the Invitation for TENDER.

26. Disclaimer:

ITI and/or its officers, employees disclaim all liability from any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of ITI and/or any of its officers, employees.

27. Accessibility of TENDER Document:

Complete Tender document with terms and conditions is provided in the following websites

- (i) <http://www.itiltd.in>
- (ii) <https://itilimited.euniwizarde.in>
- (iii) <http://eprocure.gov.in>

Annexure-I

Undertakings (To be in Bidder's Letter Head)

M/sdo here by undertake the following

1. Are not blacklisted by Central Govt./ any State or UP Govt/ PSU/ organized sector in India
2. To work with ITI as per this TENDER and Customer Tender terms and conditions. Also, we agree to implement the project (scope of work as per Tender terms and conditions including investment) covering Warranty& post-warranty services, maintenance etc, in the event of ITI winning the contract on back-to-back basis.
3. To submit Security Deposit of 5% per transaction to customer/ITI (as decided by ITI),
4. that we will be equipped with the required manpower with qualifications, certifications and experience as mentioned in the customer tender.
5. to get required certificate& support (warranty & post-warranty/maintenance) in the name of ITI from the OEM as per customer tender requirement.
6. To obtain relevant statutory licenses for operational activities.
7. to sign MoU/Teaming Agreement, Integrity Pact with ITI for addressing the customer tender as per customer's tender terms and conditions.
8. to indemnify ITI from any claims / penalties/ statutory charges, liquidated damages, with legal expenses etc as charged by the customer.
9. to support the offered equipment for a minimum period of 10 years including warranty and AMC or as per customer tender conditions.
10. To supply equipment/components which conform to the latest year of manufacture.
11. The bidder should give certificate stating that all the hardware/ software supplied under the contract shall not contain any embedded malicious codes that could inhibit the desired functions of the equipment or cause the network to malfunction in any manner.

Annexure-II

Bidders Profile

1.	Name and address of the company			
2.	Contact Details of the Bidder (Contact person name with designation, Telephone Number, FAX, E- mail and Web site)			
3.	Area of the business			
4.	Annual Turnover for financial years (Rs in Cr)	2022-23	2023-24	2024-25
5.	IT Turnover for 3 financial years (Rs in Cr)	2022-23	2023-24	2024-25
6.	Positive Net Worth as on 31.03.2025			
7.	Date of Incorporation,			
8.	GST Registration number			
9.	PAN Number			
10.	CIN Number, if applicable			
11.	Number of manpower in company's rolls			
12.	Work Experience details: Annexure IV			
13.	Certifications details like ISO or any other certification as per requirements of Customer.			

Annexure-III

Compliance Statement

Sl. No.	Clause No.	Clause	Compliance (Complied/Not Complied)	Remarks with Documentary Reference

Annexure- IV

Project Experience

Sl. No.	Name of project	Value	Name of customer	Attached Proof	Documentary

Annexure - V

INTEGRITY PACT

TENDER No.

THIS Integrity Pact is made on.....day of 2025.

BETWEEN:

ITI Limited having its Registered & Corporate Office at ITI Bhavan, Dooravaninagar, Bangalore – 560 016 and established under the Ministry of Communications, Government of India (hereinafter called the Principal), which term shall unless excluded by or is repugnant to the context, be deemed to include its Chairman & Managing Director, Directors, Officers or any of them specified by the Chairman & Managing Director in this behalf and shall also include its successors and assigns) ON THE ONE PART

AND:

..... represented by
Chief Executive Officer (hereinafter called the Contractor(s), which term shall unless excluded by or is repugnant to the context be deemed to include its heirs, representatives, successors and assigns of the contractor ON THE SECOND PART.

Preamble:

WHEREAS the Principal intends to award, under laid down organizational procedures, contract for of ITI Limited. The Principal, values full compliance with all relevant laws of the land, regulations, economic use of resources and of fairness/ transparency in its relations with its Contractor(s).

In order to achieve these goals, the Principal has appointed an Independent External Monitor (IEM), who will **monitor** the tender process and the execution of the contract for compliance with the principles as mentioned herein this agreement.

WHEREAS, to meet the purpose aforesaid, both the parties have agreed to enter into this Integrity Pact the terms and conditions of which shall also be read as integral part and parcel of the Tender Documents and contract between the parties.

NOW THEREFORE, IN CONSIDERATION OF MUTUAL COVENANTS STIPULATED IN THIS PACT THE PARTIES HEREBY AGREE AS FOLLOWS AND THIS PACT WITNESSETH AS UNDER:

SECTION 1 – COMMITMENTS OF THE PRINCIPAL

The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:

- a. No employee of the Principal, personally or through family members, will in connection with the TENDER for or the execution of the contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
- b. The Principal will, during the TENDER process treat all bidder(s) with equity and reason. The Principal will in particular, before and during the TENDER process, provide to all bidder(s) the same information and will not provide to any bidder(s) confidential/ additional information through

which the bidder(s) could obtain an advantage in relation to the TENDER process or the contract execution.

- c. The Principal will exclude from the process all known prejudiced persons. If the principal obtains information on the conduct of any of its employee, which is a criminal offence under IPC/PC Act or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary action as per its internal laid down Rules/Regulations.

SECTION 2 – COMMITMENTS OF THE BIDDER / CONTRACTOR

2.1 The Bidder(s)/Contractor(s) commits himself to take all measures necessary to prevent corruption. He commits himself observe the following principles during the participation in the TENDER process and during the execution of the contract.

- a. The bidder(s)/contractor(s) will not, directly or through any other person or firm offer, promise or give to any of the Principal's employees involved in the TENDER process or the execution of the contract or to any third person any material or other benefit which he/ she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever (during the TENDER process or during the execution of the contract).
- b. The bidder(s)/contractor(s) will not enter with other bidders/ contractors into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.
- c. The bidder(s)/contractor(s) will not commit any offence under IPC/PC Act, further the bidder(s)/contractor(s) will not use improperly, for purposes of competition of personal gain, or pass onto others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.
- d. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents /representatives in India, if any. Similarly, the Bidder(s)/Contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any.
- e. The Bidder(s) f Contractor(s) will, when presenting the bid, disclose any and all payments made, are committed to or intend to make to agents, brokers or any other intermediaries in connection with the award of the contract.
- f. The Bidder(s)/Contractor(s) will not bring any outside influence and Govt bodies directly or indirectly on the bidding process in furtherance to his bid.
- g. The Bidder(s)/Contractor(s) will not instigate third persons to commit offences outlined above or to be an accessory to such offences.

SECTION 3 – DISQUALIFICATION FROM TENDER PROCESS & EXCLUSION FROM FUTURE CONTRACTS

If the Bidder(s)/Contractor(s), during TENDER process or before the award of the contract or during execution has committed a transgression in violation of Section 2, above or in any other form such as to put his reliability or credibility in question the Principal is entitled to disqualify Bidder(s)/Contractor(s) from the TENDER process.

If the Bidder(s)/Contractor(s), has committed a transgression through a violation of Section 2 of the above, such as to put his reliability or credibility into question, the Principal shall be entitled exclude including blacklisting for future TENDER/contract award process. The imposition and duration of the exclusion will be determined by the severity of the transgression. The severity will be determined by the Principal taking into consideration the full facts and circumstances of each case, particularly taking into account the number of transgression, the position of the transgressor within the company hierarchy of the Bidder(s)/Contractor(s) and the amount of the damage. The exclusion will be imposed for a period of minimum one year.

The Bidder(s)/Contractor(s) with its free consent and without any influence agrees and undertakes to respect and uphold the Principal's absolute right to resort to and impose such exclusion and further accepts and undertakes not to challenge or question such exclusion on any ground including the lack if any hearing before the decision to resort to such exclusion is taken. The undertaking is given freely and after obtaining independent legal advice.

A transgression is considered to have occurred if the Principal after due consideration of the available evidence concludes that based on facts available there are no material doubts.

The decision of the Principal to the effect that breach of the provisions of this Integrity Pact has been committed by the Bidder(s)/ Contractor(s) shall be final and binding on the Bidder(s)/ Contractor(s), however the Bidder(s)/Contractor(s) can approach IEM(s) appointed for the purpose of this Pact.

On occurrence of any sanctions/ disqualifications etc arising out from violation of integrity pact Bidder(s)/ Contractor(s) shall not entitled for any compensation on this account.

Subject to full satisfaction of the Principal, the exclusion of the Bidder(s)/Contractor(s) could be revoked by the Principal if the Bidder(s)/ Contractor(s) can prove that he has restored/ recouped the damage caused by him and has installed a suitable corruption preventative system in his organization.

SECTION 4 – PREVIOUS TRANSGRESSION

4.1 The Bidder(s)/ Contractor(s) declares that no previous transgression occurred in the last 3 years immediately before signing of this Integrity Pact with any other company in any country conforming to the anti-corruption/ transparency International (TI) approach or with any other Public Sector Enterprises/ Undertaking in India of any Government Department in India that could justify his exclusion from the TENDER process.

4.2 If the Bidder(s)/ Contractor(s) makes incorrect statement on this subject, he can be disqualified from the TENDER process or action for his exclusion can be taken as mentioned under Section-3 of the above for transgressions of Section-2 of the above and shall be liable for compensation for damages as per Section- 5 of this Pact.

SECTION 5 – COMPENSATION FOR DAMAGE

- 5.1 If the Principal has disqualified the Bidder(s)/Contractor(s) from the TENDER process prior to the award according to Section 3 the Principal is entitled to forfeit the Earnest Money Deposit/Bid Security/ or demand and recover the damages equitant to Earnest Money Deposit/Bid Security apart from any other legal that may have accrued to the Principal.
- 5.2 In addition to 5.1 above the Principal shall be entitled to take recourse to the relevant provision of the contract related to termination of Contract due to Contractor default. In such case, the Principal shall be entitled to forfeit the Performance Bank Guarantee of the Contractor or demand and recover liquidate and all damages as per the provisions of the contract agreement against termination.

SECTION 6 – EQUAL TREATMENT OF ALL BIDDERS/CONTRACTORS

- 6.1 The Principal will enter into Integrity Pact on all identical terms with all bidders and contractors for identical cases.
- 6.2 The Bidder(s)/Contractor(s) undertakes to get this Pact signed by its subcontractor(s)/sub-empanelled partner(s)/ associate(s), if any, and to submit the same to the Principal along with the TENDER document/contract before signing the contract. The Bidder(s)/Contractor(s) shall be responsible for any violation(s) of the provisions laid down in the Integrity Pact Agreement by any of its subcontractors/ sub-empanelled partners / associates.
- 6.3 The Principal will disqualify from the TENDER process all bidders who do not sign this Integrity Pact or violate its provisions.

SECTION 7 – CRIMINAL CHARGES AGAINST VIOLATING BIDDER(S)/CONTRACTORS

- 7.1 If the Principal receives any information of conduct of a Bidder(s)/Contractor(s) or subcontractor/ sub-empanelled partner/associates of the Bidder(s)/Contractor(s) which constitutes corruption or if the principal has substantive suspicion in this regard, the principal will inform the same to the Chief Vigilance Officer of the Principal for appropriate action.

SECTION 8 – INDEPENDENT EXTERNAL MONITOR(S)

- 8.1 The Principal appoints competent and credible Independent External Monitor(s) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this pact.

Details of IEM appointed by ITI are as under:s

Name:ShriAtul Jindal IFS (Retd.),

Independent External Monitor (IEM)

Address- 3/10 VisheshKhand Opp. Little Friend School Gomti Nagar,

Lucknow-226010(UP)

E-mail: atulindia1947@gmail.com

IEM – II

Shri Benny John, IRS (Retd.),

Villa No. 36, Kent Plam Villas,

Fort Valley Township, Athani,

Kakkanad, Ernakulam,

Kerala – 682 030

- 8.2 The Monitor is not subject to any instructions by the representatives of the parties and performs his functions neutrally and independently. He will report to the Chairman and Managing Director of the Principal.
- 8.3 The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all product documentation of the Principal including that provided by the Bidder(s)/Contractor(s). The Bidder(s)/Contractor(s) will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The Monitor is under contractual obligation to treat the information and documents Bidder(s)/Contractor(s) with confidentiality.
- 8.4 The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the project provided such meeting could have an impact on the contractual relations between the Principal and the Bidder(s)/Contractor(s). As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in specific manner, refrain from action or tolerate action.
- 8.5 The Monitor will submit a written report to the Chairman & Managing Director of the Principal within toWeeks from the date of reference or intimation to him by the principal and, should the occasion arise, submit proposals for correcting problematic situations.
- 8.6 If the Monitor has reported to the Chairman & Managing Director of the Principal a substantiated suspicion of an offence under relevant IPC/PC Act, and the Chairman & Managing Director of the principal has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
- 8.7 The word 'Monitor' would include both singular and plural.

SECTION 9 - FACILITATION OF INVESTIGATION

- 9.1 In case of any allegation of violation of any provisions of this Pact or payment of commission, the

Principal or its agencies shall be entitled to examine all the documents including the Books of Accounts of the Bidder(s)/Contractor(s) and the Bidder(s)/Contractor(s) shall provide necessary information and documents in English and shall extend all help to the Principal for the purpose of verification of the documents.

SECTION 10 - LAW AND JURISDICTION

- 1.1 The Pact is subject to the Law as applicable in Indian Territory. The place of performance and jurisdiction shall be the seat of the Principal.
- 1.2 The actions stipulated in this Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

SECTION 11 – PACT DURATION

This Pact begins when both the parties have legally signed it. It expires after 1 year on completion of the warranty/ guarantee period of the project /work awarded, to the fullest satisfaction of the Principal.

If the Bidder(s)/Contractor(s) is unsuccessful, the Pact will automatically become invalid after three months on evidence of failure on the part of the Bidder(s)/Contractor(s).

If any claim is lodged/made during the validity of the Pact, the same shall be binding and continue to be valid despite the lapse of the Pact unless it is discharged/determined by the Chairman and Managing Director of the Principal.

SECTION 12 - OTHER PROVISIONS

12.1 This pact is subject to Indian Law, place of performance and jurisdiction is the Registered & Corporate office of the Principal at Bengaluru.

12.2 Changes and supplements as well as termination notices need to be made in writing by both the parties. Side agreements have not been made.

12.3 If the Bidder(s)/Contractor(s) or a partnership, the pact must be signed by all consortium members and partners.

12.4 Should one or several provisions of this pact turn out to be invalid, the remainder of this pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions

12.3 Any disputes/ difference arising between the parties with regard to term of this Pact, any action taken by the Principal in accordance with interpretation thereof shall not be subject to any Arbitration.

12.4 The action stipulates in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

In witness whereof the parties have signed and executed this Pact at the place date first done mentioned in the presence of the witnesses:

For PRINCIPAL

For BIDDER(S)/CONTRACTOR(S)

.....

.....

Name Designation

Name Designation

Witness

1.

1.

2.

2.

Appendix-B

Technical Specifications

1. 24 Port Core switch

S.No	Specifications	Compliance (Yes/No)
1	Hardware and Performance	
1.1	Switch should be fixed configuration 1 RU platform and has at least 24 Nos 10/25 Gigabit fiber ports and 4 nos. of 40G/100G Uplink ports, 1x RJ45 console port, 1x USB mini-Type B port, 1x USB Type C, 1x USB Type A port.	
1.2	Switch should have Internal redundant power supplies and hot-swappable fan tray with dual stacked fans.	
1.3	Switch should have non-blocking architecture and should support switching capacity of minimum 3.2 Tbps	
1.4	Switch should support at least 1Bpps throughput	
1.5	It should possible to connect switches in virtual stack to increase performance and active-active performance, Switch should support NSF/SSO when connected in virtual stack	
1.6	Switch should have the minimum 300000 Hrs as MTBF	
1.7	Switch should have minimum of 16 GB DRAM and 16 GB Flash memory.	
2	L2 Features	
2.1	Switch should support at least 80K Mac address	
2.2	Switch should support Ethernet standards like IEEE802.1p, IEEE802.1Q, Flow control, Jumbo frame, 802.1D, 802.1w, 802.1s, Jumbo frames, 802.3ad, private vlan	
2.3	Switch should support 4000 vlans and 1000 SVI	
2.4	Switch should support vlans based on ports, MAC address, IP-Subnet based vlan	
2.5	Switch should support CDP/LLDP, UDLD or its better equivalent protocol.	
3	L3 Features	
3.1	Switch should support 64K IPv4 and 32K IPv6 entries	
3.2	Switch should support up to 30K multicast routes	
3.3	Switch should support routing protocols like BGPv4, OSPF(v2, v3), ISISv4, RIP, Static, ECMP, LISP, VXLAN, PIM, SSM, DVMRP, BFD, VRF aware BFD	
3.4	Switch should support VRRP/HSRP	
3.5	Switch should support VRF, MPLS, Policy based routing, Network Address Translation (NAT)	
3.6	Switch should support RFC 7252 (CoAP)	
4	QoS features	
4.1	Switch should support 8 queues per port	
4.2	Switch should support IPv4 and IPv6 QoS classification and policing	
4.3	Switch should support priority queuing, DSCP, traffic shaping, WRED	

4.4	Switch should support control plane policing to protect switch CPU from DoS attack	
4.5	Switch should support IEEE 1588 and IEEE 802.1ba AV Bridging	
5	Security	
5.1	Switch should support at least 15K hardware-based ACL	
	Switch should support VLAN ACL, Port based ACL, Time based ACL	
5.2	Switch should support IP Source guard, Dynamic ARP inspection, DHCP Snooping	
5.3	Switch should support real time data collection with line rate hardware based netflow up to 64 K.	
5.4	Switch should have unique secure identity so that its authenticity and origin can be confirmed with OEM. Switch BIOS, software image should be cryptographically signed to ensure integrity and switch should not boot with modified software regardless of user's privilege level.	
5.5	Switch should support AES 256 for link encryption	
5.6	Switch should able to integrate with netflow based campus visibility and threat detection solution and should able to support threat detection within encrypted traffic.	
5.7	Switch should support RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection, IPv6 Source Guard and IPv6 Snooping	
6	Management and Troubleshooting	
6.1	Switch should support optional SSD storage, and included 240 GB or higher SSD storage to store logs and container-based application hosting	
6.2	Switch must support SD-Access architecture to enable intent-based networking, automated provisioning, and policy enforcement.	
6.3	Switch should support telnet, ssh, https, SNMPv3, IPFIX, configuration rollback feature for ease of management	
6.4	Switch should support API Driven configuration and support NETconf and RESTconf using YANG data model. It should support automation tool like python	
6.5	Switch should support port mirroring based on Inbound & outbound, mirroring based on ports, VLANS, RSPAN, ERSPAN	
6.6	Switch should support software upgrade without any downtime to network. Switch should able to support Linux based container to run applications	
6.7	Switch should support SNMP notification for dynamic change in MAC table	
6.8	Switch should support blue beacon technology to identify hardware during troubleshooting	
6.9	Switch should support AC and DC power supplies	
6.10	Switch should have field replaceable power supplies and FAN trays	
7	Switches need to be provided with all software license from day-1 as per RFP specification	
8	The switch & Transceiver module should be from same OEM.	

9	Certifications	
9.1	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.	
9.2	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or IEC/UL 62368-1 or IS 13252 Standards for Safety requirements of Information Technology Equipment.	
9.3	Switch shall conform to EN 55022 or EN 55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	
9.4	The product should have ISO 9001, ISO 14001, ISO/IEC 27001 and TEC certification.	
10	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

2. 24 port Distribution Switch

S. No	Specifications	Compliance (Yes/No)
1	Hardware and Performance	
1.1	Switch should be fixed configuration 1 RU platform and have at least 24 Nos. 10/25 Gigabit fiber ports and 4 nos. of 10G/25G Uplink ports, 1x RJ45 console port, 1x USB mini-Type B port, 1x USB Type C, 1x USB Type A port.	
1.2	Switch should have Internal redundant power supplies	
1.3	Switch should have non-blocking architecture and should support switching capacity of minimum 2 Tbps	
1.4	Switch should support at least 1Bpps throughput	
1.5	It should possible to connect switches in virtual stack to increase performance and active-active performance, Switch should support NSF/SSO when connected in virtual stack	
1.6	Switch should have the minimum 300000 Hrs as MTBF	
1.7	Switch should have minimum of 16 GB DRAM and 16 GB Flash memory.	
2	L2 Features	
2.1	Switch should support at least 80K Mac address	
2.2	Switch should support Ethernet standards like IEEE802.1p, IEEE802.1Q, Flow control, Jumbo frame, 802.1D, 802.1w, 802.1s, Jumbo frames, 802.3ad, private vlan	
2.3	Switch should support 4000 vlans and 1000 SVI	
2.4	Switch should support vlans based on ports, MAC address, IP-Subnet based vlan	
2.5	Switch should support UDLD, CDP or LLDP	
3	L3 Features	
3.1	Switch should support 64K IPv4 and 32K IPv6 entries	
3.2	Switch should support up to 30K multicast routes	
3.3	Switch should support routing protocols like BGPv4, OSPF(v2, v3), ISISv4, RIP, Static, ECMP, LISP, VXLAN, PIM, SSM, DVMRP, BFD, VRF aware BFD	
3.4	Switch should support VRRP/HSRP	
3.5	Switch should support VRF, MPLS, Policy based routing	
3.6	Switch should support RFC 7252 (CoAP)	
4	QoS features	
4.1	Switch should support 8 queues per port	
4.2	Switch should support IPv4 and IPv6 QoS classification and policing	
4.3	Switch should support priority queuing, DSCP, traffic shaping, WRED	
4.4	Switch should support control plane policing to protect switch CPU from DoS attack	
4.5	Switch should support IEEE 1588 and IEEE 802.1ba AV Bridging	

5	Security	
5.1	Switch should support at least 15K hardware-based ACL	
5.2	Switch should support VLAN ACL, Port based ACL, Time based ACL	
5.3	Switch should support IP Source guard, Dynamic ARP inspection, DHCP Snooping	
5.4	Switch should support real time data collection with line rate hardware based net flow up to 64 K.	
5.5	Switch should have unique secure identity so that its authenticity and origin can be confirmed with OEM. Switch BIOS, software image should be cryptographically signed to ensure integrity and switch should not boot with modified software regardless of user's privilege level.	
5.6	Switch should support AES 256 for link encryption	
5.7	Switch should able to integrate with net flow-based campus visibility and threat detection solution and should able to support threat detection within encrypted traffic.	
5.8	Switch should support RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection, IPv6 Source Guard and IPv6 Snooping	
6	Management and Troubleshooting	
6.1	Switch should support optional SSD storage to store logs and container-based application hosting	
6.2	Switch must support SD-Access architecture to enable intent-based networking, automated provisioning, and policy enforcement.	
6.3	Switch should support telnet, SSH, https, SNMPv3, IPFIX, configuration rollback feature for ease of management	
6.4	Switch should support API Driven configuration and support Netconf and Restconf using YANG data model. It should support automation tool like python	
6.4	Switch should support port mirroring based on Inbound & outbound, mirroring based on ports, VLANS, RSPAN, ERSPAN	
6.5	Switch should support software upgrade without any downtime to network. Switch should able to support linux based container to run applications	
6.6	Switch should support SNMP notification for dynamic change in MAC table	
6.7	Switch should support blue beacon technology to identify hardware during troubleshooting	
6.8	Switch should support AC and DC power supplies	
6.9	Switch should have field replaceable power supplies and FAN trays	
7	Switches need to be provided with all software license from day-1 as per RFP specification	
8	Certifications	
8.1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or IEC/UL 62368-1 or IS 13252 Standards for Safety requirements of Information Technology Equipment.	

8.2	Switch shall conform to EN 55022 or EN 55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	
8.3	The product should have ISO 9001, ISO 14001, ISO/IEC 27001 and TEC certification.	
8.4	Switch / Switch's Operating System should be tested for EAL2/NDPP or above under Common Criteria Certification.	
9	The switch & Transceiver module should be from same OEM.	
10	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

3. 48 Port Managed Access Switch

S. No.	Specifications	Compliance (Y/N)
1	Hardware	
1.1	Switch should be 1U and rack mountable in standard 19" rack.	
1.2	Switch should support internal field replaceable unit redundant power supply from day 1.	
1.3	Switch shall have 48 nos. 10/100/1000 Base-T ports and additional 4 Nos. 10G SFP+ uplinks ports, 1x RJ45 console port, 1x USB mini-Type B port, 1x USB Type A port.	
1.4	Switch should have minimum 4 GB DRAM and 8 GB Flash.	
1.5	Switch should have dedicated slot for modular stacking, in addition to asked uplink ports. Should support for minimum 48 Gbps of stacking throughput with 8 switch in single stack.	
2	Performance	
2.1	Switch shall have minimum 176 Gbps of switching fabric and 130 Mpps of forwarding rate.	
2.2	Switch shall have minimum 16K MAC Addresses and 250 active VLAN.	
2.3	Should support minimum 11K IPv4 routes or more	
2.4	Switch shall have 1K or more multicast routes.	
2.5	Switch should support at least 16K flow entries	
2.6	Switch should support 128 or more STP Instances.	
2.7	Switch should have 6MB or more packet buffer.	
3	Functionality	
3.1	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.	
3.2	Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1	
3.3	Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs.	
3.4	Switch shall have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.	
3.5	Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+.	
3.6	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection and IPv6 Source Guard.	
3.7	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128 on hardware for all ports.	
3.8	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.	

3.9	During system boots, the system's software signatures should be checked for integrity. System should be capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.	
3.10	The switch shall support software-defined network capabilities, including centralized policy management, automated provisioning, and network segmentation.	
4	Certification	
4.1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or IEC/UL 62368-1 or IS 13252 Standards for Safety requirements of Information Technology Equipment.	
4.2	Switch shall conform to EN 55022 or EN 55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	
4.3	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.	
4.4	The product should have ISO 9001, ISO 14001, ISO/IEC 27001 and TEC certification.	
5	All switches & Transceiver module should be from same OEM.	
6	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

4. 24 Port Managed Access Switch

S. No.	Specifications	Compliance (Y/N)
1	Hardware	
1.1	Switch should be 1U and rack mountable in standard 19" rack.	
1.2	Switch should support internal field replaceable unit redundant power supply from day 1.	
1.3	Switch shall have 24 nos. 10/100/1000 Base-T ports and additional 4 nos. 10G SFP+ uplinks ports, 1x RJ45 console port, 1x USB mini Type B port, 1x USB Type A port.	
1.4	Switch should have minimum 4 GB DRAM and 4 GB Flash.	
1.5	Switch should have dedicated slot for modular stacking, in addition to asked uplink ports. Should support for minimum 480 Gbps of stacking throughput.	
2	Performance	
2.1	Switch shall have minimum 128 Gbps of switching fabric and 95.23 Mpps of forwarding rate.	
2.2	Switch shall have minimum 16K MAC Addresses and 250 active VLAN.	
2.3	Should support minimum 11K IPv4 routes or more	
2.4	Switch shall have 1K or more multicast routes.	
2.5	Switch should support at least 16K flow entries	
2.6	Switch should support 128 or more STP Instances.	
2.7	Switch should have 6MB or more packet buffer.	
3	Functionality	
3.1	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.	
3.2	Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1	
3.3	Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs.	
3.4	Switch shall have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.	
3.5	Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+.	
3.6	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection and IPv6 Source Guard.	
3.7	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128 on hardware for all ports.	
3.8	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.	

3.9	During system boots, the system's software signatures should be checked for integrity. System should be capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.	
3.10	The switch shall support software-defined network capabilities, including centralized policy management, automated provisioning, and network segmentation.	
4	Certification:	
4.1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or IEC/UL 62368-1 or IS 13252 Standards for Safety requirements of Information Technology Equipment.	
4.2	Switch shall conform to EN 55022 or EN 55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	
4.3	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.	
4.4	The product should have ISO 9001, ISO 14001, ISO/IEC 27001 and TEC certification.	
5	All switches & Transceiver module should be from same OEM.	
6	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

5. 12 Port Managed Access switch

S. No.	General Specifications	Compliance (Yes/No)
1	Hardware :	
1.1	Switch should be 1U and rack mountable in standard 19" rack.	
1.2	Switch shall have 12 Nos. 10/100/1000 Base-T ports and additional 2 Nos of 1G Base-T and 2 nos. of 10G SFP+ uplinks ports, 1x RJ45 console port, 1x USB mini Type B port, 1x USB Type A port.	
1.3	Switch should have minimum 4 GB RAM and 4 GB Flash.	
2	Performance :	
2.1	Switch shall have minimum 68 Gbps of switching fabric and 50 Mpps of forwarding rate. Should be non-blocking and provide wire speed forwarding rate.	
2.2	Switch shall have minimum 32K MAC Addresses and 4000 VLAN IDs	
2.3	Should support minimum 14K IPv4 routes or more	
2.4	Switch shall have 1K or more multicast routes.	
2.5	Switch should support at least 16K flow entries	
2.6	Switch should support 128 or more STP Instances.	
2.7	Switch should have 6MB or more packet buffer.	
3	Functionality:	
3.1	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.1ae, 802.3u, 802.3ab, 802.3z.	
3.2	Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1.	
3.3	Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs.	
3.4	Switch shall have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.	
3.5	Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+.	
3.6	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection and IPv6 Source Guard.	
3.7	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and also have support for MACSEC-128.	
3.8	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.	
3.9	Switch should support 8 ports in a single port-channel.	
3.10	The switch shall support software-defined network capabilities, including centralized policy management, automated provisioning, and network segmentation.	
4	Certification:	

4.1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or IEC/UL 62368-1 or IS 13252 Standards for Safety requirements of Information Technology Equipment.	
4.2	Switch shall conform to EN 55022 Class A/B or EN 55032 Class A or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	
4.3	Proposed Switches and SFP transceivers should be from same OEM	
4.4	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or IS 13252 Standards for Safety requirements of Information Technology Equipment.	
4.5	Switch shall conform to EN 55022 or EN 55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	
4.6	The product should have ISO 9001, ISO 14001, ISO/IEC 27001 and TEC certification.	
4.7	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.	
5	All switches & Transceiver module should be from same OEM.	
6	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

6. 10G Single Mode SFP transceiver module

S.No	Parameter	Description	Compliance Y/N
1	Media Type:	Single-Mode Fiber (SMF)	
2	TX Wavelength:	1310 nm.	
3	RX Wavelength:	1310 nm.	
4	Minimum Optical Budget:	6 dB	
5	Maximum Distance:	10km	
6	Data Rate:	10 Gbps and should also support 1Gbps in auto negotiation	
7	Supported Applications:	10G Fiber Channel (10.52 Gbps), 8G Fiber Channel (8.5 Gbps), 4G Fiber Channel (4.25 Gbps), 2G Fiber Channel (2.125 Gbps), 1G Fiber Channel (91.0625 Gbps)	
8	DDM/DOM:	Support	
9	Temperature Range:	Standard 0°-70°C	
10	Connectors:	Double LC	
11	Tx Wavelength Bandwidth:	100 nm (1260-1360 nm)	
12	Rx Wavelength Bandwidth:	100 nm (1260-1360 nm)	
13	Minimum Transmitting Power:	-8 dB or better	
14	Maximum Transmitting Power:	-0.5 dB or better	
15	Receiver Sensitivity:	-14 dBm or better	
16	Receiver Overload:	0.5 dBm or better	
17	Dispersion:	70-100 ps/nm or better	
18	Transmitter Type:	VCSE laser/ DFB Laser	
19	Receiver Type:	PIN photodiode	
20	Power:	+3.3V single power supply	
21	Compliance:	CE, Class 1 FDA and IEC60825-1 Laser Safety Compliant, RoHS, SFF-8431, SFP MSA	
22	Warranty	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

7. 10G Multimode SFP Transceiver module

S.No	Parameter	Description	Compliance Y/N
1	Media Type:	Multi-Mode Fiber (MMF)	
2	TX Wavelength:	850 nm.	
3	RX Wavelength:	850 nm.	
4	Minimum Optical Budget:	4.6 dB	
5	Maximum Distance:	400m	
6	Supported Data Rate:	1.25-10.31 Gbps	
7	Supported Applications:	10G Ethernet (10.31Gbps), Gigabit Ethernet (1.25 Gbps), STM-64 (9.95Gbps)	
8	DDM/DOM:	Support	
9	Temperature Range:	Standard 0°-70°C	
10	Connectors:	Double LC	
11	Tx Wavelength Bandwidth:	20 nm (840-860 nm)	
12	Rx Wavelength Bandwidth:	20 nm (840-860 nm)	
13	Minimum Transmitting Power:	-6.5 dB	
14	Maximum Transmitting Power:	1 dB	
15	Receiver Sensitivity:	-11.1 dBm or better	
16	Receiver Overload:	-1 dBm or better	
17	Dispersion:	110 ps/nm or better	
18	Transmitter Type:	VCSE laser/ DFB Laser	
19	Receiver Type:	PIN photodiode	
20	Power:	+3.3V single power supply	
21	Compliance:	CE, Class 1 FDA and IEC60825-1 Laser Safety Compliant, RoHS, SFF-8431, SFP MSA	
22	Transceiver Type:	SFP+	
23	Warranty	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

8. 1G Single Mode SFP transceiver module

S.No	Parameter	Description	Compliance Y/N
1	Media Type:	Single-Mode Fiber (SMF)	
2	TX Wavelength:	1310 nm.	
3	RX Wavelength:	1310 nm.	
4	Minimum Optical Budget:	6 dB	
5	Maximum Distance:	10 km	
6	Maximum Data Rate:	1000 Mbps or higher	
7	Supported Protocol	1000 BASE-LX/LH	
8	DDM/DOM:	Support	
9	Temperature Range:	Standard 0°-70°C	
10	Connectors:	Double LC	
11	Tx Wavelength Bandwidth:	100 nm (1260-1360 nm)	
12	Rx Wavelength Bandwidth:	100 nm (1260-1360 nm)	
13	Minimum Transmitting Power:	-10 dBm or better	
14	Receiver Sensitivity:	-20 dBm or better	
15	Dispersion:	70-100 ps/nm	
16	Transmitter Type:	VCSE laser/ DFB Laser	
17	Receiver Type:	PIN photodiode	
18	Power:	+3.3V single power supply	
19	Compliance:	CE, Class 1 FDA and IEC60825-1 Laser Safety Compliant, RoHS, SFF-8431, SFP MSA	
20	Warranty	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

9. 1G Multimode SFP Transceiver module

S.No	Parameter	Description	Compliance Y/N
1	Media Type:	Multi-Mode Fiber (MMF)	
2	TX Wavelength:	850 nm.	
3	RX Wavelength:	850 nm.	
4	Maximum Distance:	400m	
5	Supported Data Rate:	1000 Mbps	
6	Supported Protocol	1000 Base- SX	
7	DDM/DOM:	Support	
8	Temperature Range:	Standard 0°-70°C	
	Connectors:	Double LC	
9	Tx Wavelength Bandwidth:	840-860 nm	
10	Rx Wavelength Bandwidth:	840-860 nm	
11	Maximum Transmitting Power:	-10 dBm or better	
12	Receiver Sensitivity:	-17dBm or better	
13	Dispersion:	110 ps/nm	
14	Transmitter Type:	VCSE laser/ DFB Laser	
15	Receiver Type:	PIN photodiode	
16	Power:	+3.3V single power supply	
17	Compliance:	CE, Class 1 FDA and IEC60825-1 Laser Safety Compliant, RoHS, SFF-8431, SFP MSA	
18	Transceiver Type:	SFP+	
19	Warranty	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

10.Next Generation Firewall

S.No	Feature	Technical Specification	Compliance (Yes/No)
1	Hardware Architecture	a) The NGFW solution must be based on dedicated hardware appliance and compatible with 19-inch Rack mountable and rack mount kit along with all accessories should be supplied along with appliance by the Bidder.	
		b) The appliance should support at least 4 x RJ45, 4 x 1G SFP ports and should be scalable to accommodate 4 x 10G for future use without changing the hardware.	
		c) The appliance hardware should be open architecture based on multi-core CPU (and not ASIC based) to protect & Scale against latest dynamic security threat. No workaround this will be accepted. The NGFW must not have any wireless interface e.g. WI-FI, Bluetooth etc.	
2	Performance & Scalability	a) The NGFW must have - Min 12 Core, Memory 64 GB RAM and 800 GB SSD storage.	
		b) The NGFW must have minimum Next Generation NGFW with IPS and Application visibility throughput of 20 9Gbps and minimum IPsec VPN throughput of 8 Gbps from Day 1.	
		c) NGFW should support at least 1.5 million concurrent sessions or more	
		d) NGFW should support at least 90 K connections per second or more	
		e) NGFW should support Active/Active or Active passive HA capability.	
3	Next Generation NGFW Capabilities	a) NGFW should support Nat66, Nat 64 & Nat46 functionality.	
		b) Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6, IGMP, PIM	
		c) The proposed NGFW should support intelligent path selection based on metric. should support PBR based on parameter likes source port, destination address, destination port, protocol, applications, or a combination of these objects. Also, PBR policy should rely on flexible metrics,	

		such as round trip time, jitter, mean opinion score, and packet loss of the interfaces to identify the best routing path for its traffic. This functionality should be provided from Day 1	
		d) Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	
		e) Must have on box Anti-virus/Anti-Malware, Anti Spyware/botnet protection signature and must have defined minimum signature update window. The NGFW must perform content-based signature matching beyond the traditional hash base signature.	
		f) Should support more than 25,000 (excluding custom signatures) IPS signatures or more to make sure that all the latest signatures are updated on the NGFW	
		g) The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor	
		h) Should must support DNS threat intelligence feeds to protect against threats	
		i) Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
		j) Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies for more than 80+ categories.	
4	Integration and Management	a) The NGFW must support to integration with Industry leading OEM NAC solution.	
		b) The NGFW manager should be a dedicated VM based appliance.	
		c) The management solution should have minimum 800 GB of more for event and	

		logging storage from day one for alert triaging	
		d) Management platform must include an integration mechanism on open standard protocol or APIs to obtain third party threat intelligence data from other devices e.g. NAC, WAF, SIEM etc. on malicious IPs, URLs and Domains and define & execute firewall policy to block those malicious attributes and list must get updated dynamically with latest data.	
		e) Should support XML/ RESTful API to integrate with network management and monitoring systems.	
		f) Must support device management and NGFW policies using local console, CLI (SSH) , GUI management Interface	
5	Certification	The product should have ISO certification, BIS certification, RoHS compliance, Cert-in registration certification	
6	Warranty & OEM Support	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

11. Network Access Control Appliances

S.No	Specifications	Compliance
1	General Hardware	
1.1	The proposed solution should be available on Hardware	
1.2	The proposed solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture; Guest; profiling; and BYOD services on a single platform.	
1.3	The proposed solution should control access to the network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices.	
1.4	The proposed solution should provide 600 GB HDD Storage	
1.5	The proposed solution should have a Centralized Management Console with customizable dashboard and role-based admin. Solution should enables administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, greatly simplifying administration by providing consistency in managing all these services.	
1.6	The proposed solution should operate within a heterogeneous network with switches, routers, etc. from multiple vendors. NAC appliance should support vendor agnostic switch infrastructure.	
1.7	The proposed solution should allow to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise.	
1.8	The proposed solution should provide comprehensive visibility of the network by automatically discovering, classifying, and enforcing policy for endpoints connected to the network and must have capacity to enable the appropriate services for at least a total of 1000 endpoint devices.	
1.9	The proposed solution should support on-demand health-check of the hardware nodes.	
1.10	The proposed solution should support the backup and recovery of policies/configuration.	
1.11	The proposed solution should support consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed	
1.12	The proposed solution should support Federal Information Processing Standard (FIPS) 140-2 or equivalent Indian standard	
1.13	The proposed solution should support remote access capabilities on its management interface via HTTPS or SSH access	
1.14	The proposed solution must support a managed switch environment having 802.1 x support.	
1.15	Should support multiple Admin Group Roles and responsibilities like HelpDesk Admin, Identity Admin, Monitoring Admin, Network Device Admin, Policy Admin, RBAC Admin, Super Admin, Read-Only Admin and System Admin	

1.16	The proposed solution to be in High availability so that even if one appliance/server fails, the other server takes over.	
1.17	The proposed solution should have capability to send alerts regarding the health of the solution through emails.	
1.18	The proposed solution should support API ERS and Open API	
2	Radius / Dot1x / AAA	
2.1	The proposed solution should be able to control the user even before IP address is assigned. It should act as a pre-admission solution	
2.2	The proposed solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), TEAP, and EAP-Transport Layer Security (TLS).	
2.3	The solution should provide a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	
2.4	The Solution should support Certificate Fingerprinting to evaluate Certificate issuer SHA-256 in policies.	
2.5	The proposed solution should have capability to assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).	
2.6	The proposed solution should be capable of being by passed in the event of any failure of the solution.	
2.7	The proposed solution should be able to control Maximum concurrent sessions per user/group	
2.8	The solution should be able to block unauthenticated/rogue machine without giving any access to the network.	
2.9	The proposed solution should support Real time Policy hit counts	
3	Guest	
3.1	The proposed solution should provide complete guest lifecycle management by empowering admin to on-board guests.	
3.2	The proposed solution should provide feature for admin to extend, terminate & manage password for the registered guest.	
3.3	The portal used for Device registration should be customizable, allowing to customize portal theme by changing text, banners, background color, and images	
3.4	The proposed solution should support multiple guest types to differentiate between external guest based on time period for which the account is created for.	
3.5	The proposed solution should have provision for admin to approve the request coming from external guest and after approval the credentials will be shared.	
3.6	The proposed solution should have provision to provide grace period to guest till the time admin approves the request.	
3.7	The proposed solution should support testing of the Guest portal before pushing it into production.	

3.8	The proposed solution should have provision to customise the Guest portal with Logos and text.	
4	Posture	
4.1	The proposed solution should automatically enforce security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area with appropriate notifications to the administrator	
4.2	The proposed solution should support running custom scripts to remediate non-compliant endpoints.	
4.3	The solution should provide granular compliance checks for Windows, MAC and Linux in terms of: - Check operating system, service packs, hotfixes - Check process, registry, file & application - Check for Antivirus installation, Version, Antivirus Definition Date - Check for Antispyware installation, Version, Antispyware Definition Date - Check for windows update running & configuration - Ability to run custom scripts and policies	
4.4	The proposed solution should permit admin to define thresholds for Anti-Virus Definition checks, if definition is not updated then Endpoint should be blocked.	
4.5	The proposed solution must be able to integrate with Endpoint Patch management such as WSUS for Auto or Manual Remediation	
4.6	The proposed solution should provide automatic remediation.	
4.7	The proposed solution should update the latest definition and product versions automatically.	
4.8	The proposed solution should permit configuring baseline version of the AV/AM to be checked on the endpoints.	
5	Device Profiling	
5.1	The proposed solution should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, laptops, desktops and workstations.	
5.2	The proposed solution should allow Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type.	
5.3	The proposed solution should have capability to see endpoints attribute data via passive network telemetry or alternatively from the infrastructure via device sensors on switches at Core, Distribution and Access Layer.	

5.4	The solution should have profiling capabilities integrated into the solution in order to detect headless host. The profiling features leverage the existing infrastructure for device discovery. Should support the use of attributes from the following sources or sensors: - Profiling using MAC OUIs - Profiling using DHCP information - Profiling using RADIUS information - Profiling using HTTP information - Profiling using DNS information - Profiling using NetFlow information - Profiling using SPAN/Mirrored traffic	
5.5	The proposed solution should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma.	
5.6	The proposed solution should have capability to combine multiple profiles of similar endpoints into single logical profile	
6	Certificate authority (CA)	
6.1	The solution must have internal CA server functionality with flexibility to create certificate template to be used by other network services	
6.2	The proposed solution should have capability to revoke the issued certificate.	
6.3	The CA server should be able to provision certificate for multiple use cases like BYOD, EAP authentication and Third Party Client and Server side authentication.	
6.4	The proposed solution should have capability to integrate with External CA for issuing the certificates	
7	External Identities	
7.1	The proposed solution should support configuring multiple Identity sources to validate for user credentials. Solution should support the following databases: •Internal Users •Internal Endpoints •Active Directory •LDAP •RSA •RADIUS Token Servers •ODBC •Certificate Authentication Profiles	
7.2	The proposed solution should support configuring Multiple Active Directory Domains for Authentication of User Credentials.	
7.3	The proposed solution should support enabling or disabling authentication towards any child domain that is part of the same forest.	

7.4	The Solution should support MSRPC protocol for pulling Login information from Active Directory to be used for Authentication of Endpoints.	
7.5	The proposed solution should have capability to re-write the incoming Identity to a different format which LDAP/Active directory understands.	
8	Intergration	
8.1	Solution should support 3rd party integration for sharing Contextual awareness and other endpoint related data such that it can Publish, subscribe and work as broker as well.	
8.2	The proposed solution should be able to integrate with Firewall to create more granular policies.	
8.3	Reporting & Troubleshooting	
8.4	The proposed solution shall monitor, detect, alert, report and provide remediation for any unauthorized access.	
8.5	The proposed solution should be supported to integrate with Enterprise level SIEM solutions to forward all the logs and events.	
8.6	The proposed solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting.	
8.7	The proposed solution should have extensive troubleshooting capabilities to collect packet captures, debugs particular endpoint , run commands on switch to collect information to provide visibility for an administrator.	
8.8	The proposed solution should have built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.	
9	TACACS+ (Device Administration)	
9.1	The proposed should support TACACS+ protocol for authorization of each command executed on the shell of the routers & switches.	
9.2	For the proposed TACACS+ service , Vendor solution should not charge for number of network devices or number of device administrators.	
9.3	The proposed solution must have workflow for Device Administration Policy to guide the admins through different phases as follows: 1. Prepare (authorization roles; Authorization permissions/privileges, command sets that administrator may perform, Activation of TACACS+ feature) 2. Define (Add network devices - router/firewalls/switches/proxy/WAF/WLCs etc. with TACACS+ secret keys, Group/Users who wil perform device administration - internal/external,MFA/2FA, Different Policy where profile and command sets are applied)	

	3. Go Live and Monitor (Monitor events/Live Logs and Examine Reports to check access and authorization is as intended)	
9.4	The proposed solution should support different conditions for TACACS+ or Device Administration Policy - 1. Device Network Condition(IP Address/ Device type/ Device Group) 2. Device Port condition (IP Address, Device, Network Device Group/Port used) 3. Simple/Compund Condition - EndUser/EndUser Group/Time of the day/office hours etc)	
9.5	The proposed solution should log below field for the Commands 1. User who has given Command on Element 2. Date of Command given 3. Time of Command given 4. Actual Command given from IP Address.	
9.6	Basis of different conditions for TACACS+ or Device Administration, solution should support results as TACACS+ Profiles and command sets.	
9.7	TACACS+ profiles should support shell profiles - Privilege levels (default, Maximum), Access control List, auto commands, no escape, timeouts and Idle timeouts as actions.	
9.8	The proposed solution should support Posture check and 802.1x authentication using a single endpoint agent.	
9.9	TACACS+ profiles should support profile for WLC with permissions - all, monitor, lobby or selected roles/tabs like only WLAN, controller, wireless, Security, Management or commands	
9.10	TACACS+ profiles should support profile for Nexus and Generic devices	
9.11	TACACS+ command sets should come with prebuilt command set profiles for deny all commands, allow all commands and show only commands.	
9.12	TACACS+ command sets should allow to define custom command sets with options to list the permitted command or negate option to not allow any other command that is not listed in the command set.	
9.13	TACACS+ command set should support following actions or permissions - PERMIT/ALLOW, DENY/BLOCK, DENY ALWAYS/BLOCK ALWAYS or equivalent actions	
9.14	TACACS+ command set should support action with command along with the arguments of the command that administrator is allowed to execute.	
9.15	TACACS+ service should allow authentication via. External TACACS+ / RADIUS Proxy or RADIUS Token server but authorization and accounting done locally.	
9.16	TACACS+ service should support custom settings for - Protocol session timeout, connection timeout, packet size, authorization cache timeout, customer username and password prompt, password change, Password Violation policy prompt etc.	

9.17	TACACS+ Authentication settings should support TACACS Compliance Single Connect Support	
9.18	TACACS+ External authentication settings should support provision for stripping username prefix such as backslash (\) or stripping of the suffix at the rate (@) with provision to handle the accounting request for TACACS+ session locally or remotely.	
9.19	TACACS+ service reports should include at least following - Authentication summary for T+ based authentications, TACACS+ Accounting TACACS+ Authorization, TACACS+ command Accounting, Top N Authentication by failure Reasons, Top N Authentications by Network Devices and Top N Authentication by Users report. Also should support scheduling of the report and provision to create and export - default/custom reports.	
9.20	Solution should have provision to keep passwords entered accidentally in username fields hidden for audit and security purpose. Wrong values in username field should reflect generic keyword USERNAME	
9.21	The proposed solution should provide complete guest lifecycle management by empowering sponsors to on-board guests.	
10	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

12. Software Defined Network (SDN) controller appliance

Sl. No.	Item Specifications	Compliance (Yes/No)
1	General Features	
1.1	Architecture: The SDN device must be based on an open architecture that allows for flexibility and scalability. It should support a centralized control plane with distributed data planes and support existing customer computer network	
1.2	Form Factor: 1U rack-mountable chassis compatible with standard 19" racks.	
1.3	Power Supply: Hot-swappable, redundant internal power supplies for enhanced reliability.	
1.4	Memory: Minimum 16 GB RAM and 32 GB Flash storage.	
1.5	Storage: Minimum 800 GB SSD for logging and event storage.	
2	Performance	
2.1	Throughput: Minimum throughput of 20 Gbps for data processing and management operations.	
2.2	Session Handling: Capable of handling at least 4 million concurrent sessions.	
2.3	Connection Rate: Supports at least 170,000 connections per second.	
2.4	Scalability: Should support a network scale of up to 300 devices (switches and routers) and 1200 endpoints.	
3	SDN Controller Features	
3.1	Centralized Management: The SDN controller must provide a single dashboard for centralized management, including device lifecycle management, topology discovery, inventory management, and image upgrades.	
3.2	Zero Touch Provisioning (ZTP): Support for automated onboarding and configuration of network devices from their factory-default state.	
3.3	Policy Management: Ability to define and enforce network policies based on user roles, applications, and device types.	
3.4	Dynamic Discovery: Support for LLDP, SNMP, IPDT, and ARP for host discovery and network topology mapping.	
4	Automation and Orchestration	
4.1	Automation Capabilities: The SDN solution should enable true automation of network operations, including configuration of overlay and underlay networks.	
4.2	Self-Learning: The solution must have self-learning capabilities to discover devices and optimize configurations based on network conditions	
4.3	Automated Fault Management: Should include mechanisms for automated fault detection and remediation to minimize downtime.	
4.4	Remote Management Assistance (RMA): Support for multiple vendors	
5	Visibility and Insights	

5.1	Traffic Monitoring: Provide comprehensive visibility into network traffic, including application visibility using Deep Packet Inspection (DPI).	
5.2	Device Assurance and Provisioning: SDN Solution have capability of Device On Boarding process	
5.3	Endpoint Device Management: Solution should provide End Point OS level information, location and User based information	
5.4	Health Monitoring: Capabilities to monitor the health of network devices, clients, and applications with metrics such as latency and packet loss.	
5.5	Alerting and Reporting: The system should generate alerts for network issues categorized by criticality (P1, P2, P3) and provide detailed reports on device performance, compliance, and security.	
6	Security Features	
6.1	Integration with NAC: The SDN device must support integration with Network Access Control (NAC) solutions for enhanced security.	
6.2	Micro-Segmentation: Capability to create network segments based on user roles and apply specific policies to each segment.	
6.3	Policy Compliance: Continuous monitoring for policy compliance, with automatic SNMP traps for configuration changes.	
7	Compliance and Standards	
7.1	Standards Compliance: Must comply with relevant industry standards, including IEEE 802.1 standards for Ethernet and security protocols.	
7.2	Cryptographic Integrity: All firmware and software images must be cryptographically signed to ensure authenticity and integrity.	
8	Management and Troubleshooting	
8.1	SIEM Support: Solution should have SIEM feature	
8.2	Automation: Job Scheduling (Configuration changes, OS and Patch Updates)	
8.3	Management Interfaces: Support for SSH, SNMPv3, and web-based management interfaces.	
8.4	API Support: Must support XML/RESTful APIs for integration with third-party management systems and automation tools.	
8.5	Logging and Monitoring: Capabilities for real-time logging with support for Syslog and other logging protocols.	
9	Support and Warranty	
9.1	Warranty: 3 years onsite comprehensive OEM warranty, 24x7 OEM TAC support	
9.2	Hardware Replacement: Next Business Day hardware replacement for critical components.	
10	Additional Features	
10.1	Granular Visibility: The solution should provide detailed visibility into power consumption for endpoint devices and switches.	
10.2	Integration with Third-Party Solutions: The SDN device must support integration with third-party applications using Northbound REST APIs.	

13.86" Display for Network monitoring

S. No.	Parameter	Specification	Compliance
1	Screen Size (Diagonal)	86" or more	
2	Panel Type	IPS/VA	
3	Resolution	3840x2160	
4	Lifetime (Typical)	50000 Hours	
5	Contrast ratio	5000:1	
6	Dynamic Contrast Ratio	30000:1	
7	Brightness	At least 450 nits (with glass)	
8	Touch Type	IR	
9	Touch Accuracy	Equal to or less than +/- 1 mm	
10	Display response time	8 ms	
11	Touch Response	Less than or equal to 8 ms	
12	No. of Touch Points	At least 40	
13	RAM and ROM	Minimum 4 GB and Minimum 32 GB	
14	Processor	Quad Core	
15	Surface Thickness	Should be atleast 4 mm	
16	Hardness (Mohs)	Should be atleast 9H	
17	I/O Ports	HDMI (3 nos. IN and 1 no. Out), DP IN, VGA In, Audio In/Out, SPDIF (Optical Audio Out), RJ 45, USB 3.0 - 4 nos., USB 2.0- 4 nos., Touch USB 2 no., OPS Slot, RS 232, USB C type port with 65W Charging	
18	Network port in Display	Should be 10/100/1000 MBPS	
19	Operation Hours	At least 18/7	
20	Built in speaker	16W x 2	
21	Builtin OS	Android 11 or higher version	
22	Health Related Features	Blue Light Filter certified by TUV Rhineland, Certificate to be produced, Flicker Free certified by certified by TUV Rhineland, Certificate to be produced, Anti Glare certified by certified by TUV Rhineland, Certificate to be produced	
23	Device Management Services	Should be preinstalled by default in IFP for Centralized management tool to manage all the IFP in the network, Should have dashboard view and able to control and toggle display setting and operate remotely. Should be from the same OEM. Should be perpetual based without any year on year subscription	
24	Annotation Tool	Should be able to Annotate on screen with tools like Pen, Eraser, Partial Capture, Annotate on running video, Screen Recording	

25	Shortcuts	Should be able to create shortcuts of apps installed in IFP	
26	Document Read/ Write	Should be able to Open and edit documents like MS Word, Excel, PPT. Should be able to open PDF Documents	
27	Additional features	Temperature Sensor, Auto Brightness Sensor, Tile Mode (up to 15x15), Natural Mode@Tile Mode, ISM Method, Internal Memory, Wi- Fi built-in, USB Cloning, Contents Scheduling, Sync mode, PM mode, Fail Over, Wake on LAN, BEACON (On/Off), Embedded Template	
28	IFP-OEM should have valid certificates:	Valid ISO 9001, 14001and 45001, ROHS Certification, BIS, CE,CB,FCC, TUV certification for Blue Light Filter and Flicker Free, Certification for Germ Resistant Coating SIAA KOHKIN	
29	Input devices	USB keyboard and USB mouse should be included in the supply	
30	Warranty	Warranty: 3 years onsite comprehensive OEM warranty and 24x7 OEM Technical Assistance Centre (TAC) support.	

14. Cat6 UTP Cable.

S. No.	Parameter	Specification	Compliance (Yes/No)
1	Product Code / Recommended Make	To be Specified by the Bidder	
2	Type	CAT6 U/UTP LSZH Cable	
3	Type	23 AWG solid bare copper, Unshielded Twisted 4 Pair, Category 6, confirming to ANSI-TIA 568.2-D for Category 6 & ISO/IEC 11801 for Class E.	
4	Conductors	Solid bare copper 23 AWG	
5	Pair Separator	+ Shape Spline	
6	Cable length	305 meters UTP cable packed in roll box	
7	Cable Outer Diameter	6.0 ± 0.2 mm	
8	Delay Skew	< 45 ns	
9	Conductor Resistance	≤ 93.8 Ω/km	
10	Pulling Force	25 lb	
11	Nom. Velocity of Propagation	69%	
12	Temperature Range Storage	-20 °C to +70 °C	
13	Flame Properties	Flammability Test : IEC 60332-1	
		Acid Gas Emission Test : IEC 60754-1	
		Smoke Density Test : ASTM 2843	
14	Regulatory Compliances	Should be ETL channel performance verified on a 04-Connector channel or more, tested upto 700Mhz with an MTPL Plug as per ANSI/TIA-568.2-D (Part Code to be mentioned in report and should be submitted along with bid) and UL Listed (Relivent Document to be shared)	
15	RoHS Compliant	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	

15. Cat6 Unshielded LSZH Patch Cords with 1 meter length

S. No.	Parameter	Specification	Compliance (Yes/No)
1	Product Code / Recommended Make	To be Specified by the Bidder	
2	Type	CAT6 Unshielded LSZH Patch Cord Cable	
3	Patch cord colour	Yellow/ Blue	
4	Type	Modular Cord shall meet and exceed channel specification of ANSI/TIA 568.2-D, ISO/IEC 11801 Class E & IEC 61156-6 Standard.	
5	Conductor	Flexible Stranded Bare Copper, 24 AWG	
6	Insulation / Diameter	PE (0.95 ± 0.05 mm)	
7	Feature	Transparent Strain Relief easy latch-cover boot design for easy depression	
		Backward compatible for easy integration with any network component that uses a RJ45 connection	
8	Length	1 meter	
9	Connectors	High Grade 50 µ gold plated RJ45 Connectors	
10	Conductor Material	Stranded Bare Copper	
11	Storage Temperature Range :	-20 °C to +70°C	
12	Sheath Material	LSZH	
13	Cable Diameter	5.86 ± 0.3mm	
14	Electrical Specification :	Conductor DC Resistance : 14Ω / 100m	
		Resistance Unbalance : 50mΩ	
		Impedance : 100Ω ± 15%	
		Frequency : 250MHz Maximum	
		Insulation Resistance (Max) : 376 Ω/Km	
		Delay Skew : 45ns/100m	
15	Performance	Patch Cords which will give guaranteed higher bandwidth will be preferred.	
16	Regulatory Compliances	Should be ETL Channel performance verified on a 04-Connector channel or more, tested upto 635Mhz with an MTPL Plug as per ANSI/TIA-568.2-D (Part Code to be mentioned in report and should be submitted along with bid) and UL Listed (Relivent Document to be shared)	
17	RoHS Compliant	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	

16. Cat6 Unshielded LSZH Patch Cords with 2-meter length

S. No.	Parameter	Specification	Compliance (Yes/No)
1	Product Code / Recommended Make	To be Specified by the Bidder	
2	Type	CAT6 Unshielded LSZH Patch Cord Cable	
3	Patch cord colour	Yellow/ Blue	
4	Type	Modular Cord shall meet and exceed channel specification of ANSI/TIA 568.2-D, ISO/IEC 11801 Class E & IEC 61156-6 Standard.	
5	Conductor	Flexible Stranded Bare Copper, 24 AWG	
6	Insulation / Diameter	PE (0.95 ± 0.05 mm)	
7	Feature	Transparent Strain Relief easy latch-cover boot design for easy depression	
		Backward compatible for easy integration with any network component that uses a RJ45 connection	
8	Length	2 meter	
9	Connectors	High Grade 50 µ gold plated RJ45 Connectors	
10	Conductor Material	Stranded Bare Copper	
11	Storage Temperature Range :	-20 °C to +70°C	
12	Sheath Material	LSZH	
13	Cable Diameter	5.86 ± 0.3mm	
14	Electrical Specification :	Conductor DC Resistance : 14Ω / 100m	
		Resistance Unbalance : 50mΩ	
		Impedance : 100Ω ± 15%	
		Frequency : 250MHz Maximum	
		Insulation Resistance (Max) : 376 Ω/Km	
		Delay Skew : 45ns/100m	
15	Performance	Patch Cords which will give guaranteed higher bandwidth will be preferred.	
16	Regulatory Compliances	Should be ETL Channel performance verified on a 04-Connector channel or more, tested upto 635Mhz with an MTPL Plug as per ANSI/TIA-568.2-D (Part Code to be mentioned in report and should be submitted along with bid) and UL Listed (Relivent Document to be shared)	
17	RoHS Compliant	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	

17.12F 1U Rack Mount Fiber Enclosure (LIU) including Splice Trays, pigtails and couplers

S. No.	Parameter	Specification	Compliance (Yes/No)
1	Product Code / Recommended Make	To be Specified by the Bidder	
2	Type	1U Rack Mount Fiber Enclosure (LIU) including Splice Trays and Adapter Strips which accepts loose tube & distribution cable	
3	Fiber Interface Unit	Fiber Patch Panel Typically used in Server rooms, Network rooms, Data Centres and Small offices Can be mounted directly on any 19" rack or cabinet. It should be able to accommodate a variety of Fiber connectors and terminated to fiber cables using Splicing or other methods.	
4	Type	Fiber LIU should be 1U, 19 Inch Rack Mount.	
		12/24 Port should be available in 1U Rack Mount LIU.	
5	Features & Compatibility	The Fiber Panels are designed with fixed mount adapter plate assemblies.	
		Sliding design, this panel allows easy access during installation or rework without disturbing previously terminated fiber cable.	
		This also offers multiple cable entries to provide various customized solutions as per the customers' requirement.	
		This panel comes with adaptor plates which are preloaded with coupler and can snap in for installation and can be removed easily for future changes.	
		900m Tight buffer pigtails are provided with this panel. This panel is preloaded with Splice tray & necessary fiber management accessories.	
		4 Nos of 20mm diameter at the rear for Cable entries	
6	Material	Panel be constructed with SPCC (Cold rolled steel sheet)	
7	Standards	Conformance to Single Mode (ANSI/TIA-568.3-D, Telcordia GR-326-CORE, Telcordia GR-1221-CORE, ISO/IEC 11801, IEC 61754 & IEC 61300 series), Multi Mode (ANSI/TIA-568.3-D, IEC 61300-3-4, IEC 61300-3-6, IEC 60874-1, ISO/IEC 11801)	

8	Adapter Types	Pigtails consist of LC, SC, FC, ST, MTRJ, and E2000 Connectors.	
9	Pigtails Type	Pigtails shall be constructed with bend Insensitive Fiber	
10	Insertion Loss	≤ 0.2 dB (Single mode) , ≤ 0.3 dB (Multimode)	
11	Return Loss	≥ 50 dB (UPC), (Single mode) , ≥ 60 dB (APC) (Single mode), ≥ 35 dB (UPC) (Multimode),	
12	Repeatability	≤ 0.1 dB	
13	Durability	≤ 0.2 dB, 1000mattings	
14	Ferrule Material	Zirconia Ceramic	
15	Operating Temperature	-25 °C to +70 °C	
16	Regulatory Compliances/Certifications	OEM should be an ISO9001, ISO 14001 and ISO 45001 should have its Manufacturing units, Components and Finished Goods Warehouse & R&D labs in India. The OEM shall be CE Certified. All Related documents to be submitted.	
		The system integrator should be certified by the proposed OEM and shall be having 04 certified engineer on the same. (Documents to be enclosed)	
		OEM offered must be in India / SAARC for at-least 10 years or more. Should have Indian Technical Support Centre, Warehouse and RMA centre in India.	
17	RoHS Compliant	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	

18. 48F 1U Rack Mount Fiber Enclosure (LIU) including Splice Trays, pigtails and couplers

S. No.	Parameter	Specification	Compliance (Yes/No)
1	Product Code / Recommended Make	To be Specified by the Bidder	
2	Type	1U Rack Mount Fiber Enclosure (LIU) including Splice Trays and Adapter Strips which accepts loose tube & distribution cable	
3	Fiber Interface Unit	Fiber Patch Panel Typically used in Server rooms, Network rooms, Data Centres and Small offices Can be mounted directly on any 19" rack or cabinet. It should be able to accommodate a variety of Fiber connectors and terminated to fiber cables using Splicing or other methods.	
4	Type	Fiber LIU should be 1U, 19 Inch Rack Mount.	
		48 Port should be available in 1U Rack Mount LIU.	
5	Features & Compatibility	The Fiber Panels are designed with fixed mount adapter plate assemblies.	
		Sliding design, this panel allows easy access during installation or rework without disturbing previously terminated fiber cable.	
		This also offers multiple cable entries to provide various customized solutions as per the customers' requirement.	
		This panel comes with adaptor plates which are preloaded with coupler and can snap in for installation and can be removed easily for future changes.	
		900m Tight buffer pigtails are provided with this panel. This panel is preloaded with Splice tray & necessary fiber management accessories.	
		4 Nos of 20mm diameter at the rear for Cable entries	
6	Material	Panel be constructed with SPCC (Cold rolled steel sheet)	
7	Standards	Conformance to Single Mode (ANSI/TIA-568.3-D, Telcordia GR-326-CORE, Telcordia GR-1221-CORE, ISO/IEC 11801, IEC 61754 & IEC 61300 series), Multi Mode (ANSI/TIA-568.3-D, IEC 61300-3-4, IEC 61300-3-6, IEC 60874-1, ISO/IEC 11801)	

8	Adapter Types	Pigtails consist of LC, SC, FC, ST, MTRJ, and E2000 Connectors.	
9	Pigtails Type	Pigtails shall be constructed with bend Insensitive Fiber	
10	Insertion Loss	≤ 0.2 dB (Single mode) , ≤ 0.3 dB (Multimode)	
11	Return Loss	≥ 50 dB (UPC), (Single mode) , ≥ 60 dB (APC) (Single mode), ≥ 35 dB (UPC) (Multimode),	
12	Repeatability	≤ 0.1 dB	
13	Durability	≤ 0.2 dB, 1000mattings	
14	Ferrule Material	Zirconia Ceramic	
15	Operating Temperature	-25 °C to +70 °C	
16	Regulatory Compliances/Certifications	OEM should be an ISO9001, ISO 14001 and ISO 45001 should have its Manufacturing units, Components and Finished Goods Warehouse & R&D labs in India. The OEM shall be CE Certified. All Related documents to be submitted.	
		The system integrator should be certified by the proposed OEM and shall be having 04 certified engineer on the same. (Documents to be enclosed)	
		OEM offered must be in India / SAARC for at-least 10 years or more. Should have Indian Technical Support Centre, Warehouse and RMA centre in India.	
17	RoHS Compliant	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	

19.LC-LC Duplex Single mode Fiber patch cord

S.No	Specification	Description	Compliance
1	Fiber Type	Single-Mode (SM)	
2	Length	3 meters (300 cm) or more	
3	Fiber Core Diameter	9/125 μm (Standard for single-mode fiber)	
4	Cladding Diameter	125 μm	
5	Outer Jacket Material	LSZH (Low Smoke Zero Halogen)	
6	Jacket Color	Yellow	
7	Cable Type	Duplex	
8	Connector Types	LC-LC	
9	LC Connector Polish Type	UPC (Ultra Physical Contact) / APC (Angled Physical Contact)	
10	SC Connector Polish Type	UPC (Ultra Physical Contact) / APC (Angled Physical Contact)	
11	Ferrule Material	Ceramic (zirconia)	
12	Insertion Loss (IL)	≤ 0.3 dB (Typical)	
13	Return Loss (RL)	≥ 50 dB for UPC, ≥ 60 dB for APC	
14	Durability	> 1000 mating cycles	
15	Attenuation	≤ 0.4 dB/km at 1310 nm, ≤ 0.3 dB/km at 1550 nm	
16	Bandwidth	≥ 100 MHz·km at 1310 nm	
17	Maximum Tensile Strength	80 N (depending on cable construction)	
18	Operating Temperature Range	-20°C to 70°C	
19	Storage Temperature Range	-40°C to 85°C	
20	Bending Radius (Static)	≥ 20 mm (LC connectors), ≥ 30 mm (SC connectors)	
21	Bending Radius (Dynamic)	≥ 10 x cable diameter	
22	Flammability Rating	UL 94-V0 (for LSZH cables)	

23	Compliance & Standards	ISO/IEC 11801, TIA/EIA-568-C	
24	Compliance & Standards	ISO/IEC 11801, TIA/EIA-568-C	
25	Polarity	Standard polarity A to B, and B to A	
26	Certifications	RoHS compliance, CE certification, REACH compliant	

20. LC-LC Duplex Multimode fiber patch cord.

S.No	Specification	Description	Compliance
1	Fiber Type	Multimode (MM)	
2	Length	3 meters	
3	Fiber Core Diameter	50/125 μm or 62.5/125 μm (depending on multimode fiber type)	
4	Cladding Diameter	125 μm	
5	Outer Jacket Material	LSZH (Low Smoke Zero Halogen)	
6	Jacket Color	Orange/ Aqua	
7	Cable Type	Duplex	
8	Connector Types	LC-LC	
9	LC Connector Polish Type	UPC (Ultra Physical Contact) /APC (Angled Physical Contact)	
10	SC Connector Polish Type	UPC (Ultra Physical Contact) / APC (Angled Physical Contact)	
11	Ferrule Material	Ceramic (zirconia)	
12	Insertion Loss (IL)	≤ 0.3 dB (Typical)	
13	Return Loss (RL)	≥ 30 dB for UPC, ≥ 50 dB for APC	
14	Durability	> 1000 mating cycles	
15	Attenuation	≤ 3.5 dB/km at 850 nm, ≤ 1.0 dB/km at 1300 nm (OM1); ≤ 1.5 dB/km at 850 nm, ≤ 0.5 dB/km at 1300 nm (OM2); ≤ 0.3 dB/km at 850 nm, ≤ 0.3 dB/km at 1300 nm (OM3/OM4)	
16	Bandwidth	OM3/OM4: ≥ 2000 MHz·km at 850 nm	
17	Maximum Tensile Strength	80 N or better	
18	Operating Temperature Range	-20°C to 70°C	
19	Storage Temperature Range	-40°C to 85°C	
20	Bending Radius (Static)	≥ 20 mm (LC connectors), ≥ 30 mm (SC connectors)	

21	Bending Radius (Dynamic)	$\geq 10 \times$ cable diameter	
22	Flammability Rating	UL 94-V0	
23	Compliance & Standards	ISO/IEC 11801, TIA/EIA-568-C	
24	Polarity	Standard polarity A to B, and B to A	
25	Certifications	RoHS compliance, CE certification, REACH compliant	

21. 12F Core Single mode Fiber Optic Cable.

S. No.	Parameter	Specification	Compliance (Yes/No)
1	Product Code / Recommended Make	To be Specified by the Bidder	
2	Type	12F Core Single mode (9/125 μ m) G652 Fiber optic Outdoor Cable	
3	Cable	12F Core Single Mode Unloose Tube, Single Sheath, Fiber cable is perfectly suited for both gigabit Ethernet and 10/25 gigabit Ethernet campus and backbone applications	
4	Application	Should be suitable for both gigabit Ethernet and 10/25 Gigabit ethernet campus and backbone networking applications.	
5	Outer Sheath	UV Resistance HDPE Jacket / Black	
6	No. of Tube / Tube diameter	1 / 3.0 $\pm$ 0.1 mm	
7	Water Blocking Material	WS Tape	
8	Loose Tube Construction	Std. plywood reel: Uniloose Tube, Water Blocking with fibres. Individually colour coded optical fibres as per Global Standards	
9	Cable Specifications	Fiber Color / Fibers per Tube : Blue, Orange, Green, Brown, Grey, White, Red, Black, Yellow, Violet, Pink, Aqua Cable diameter : 9.0 $\pm$ 0.5 mm	
10	Optical Properties	Core Non-circularity : $\leq$ 1 %	
		Cladding Diameter : 125.0 $\pm$ 0.7 μ m	
		Core/cladding Concentricity Error : $\leq$ 0.6 μ m	
		Cladding Non-circularity : $\leq$ 1.0 %	
		Primary Coating Diameter : 245 $\pm$ 10 μ m	
		Coating/cladding Concentricity Error : $\leq$ 12 μ m	
		Attenuation Co-efficient	
		1310 Wavelength (nm) : $\leq$ 0.36 dB/km	
		1550 Wavelength (nm) : $\leq$ 0.24 dB/km	
		1625 Wavelength (nm) : $\leq$ 0.26 dB/km	
		Chromatic dispersion :	
		1285 ~ 1330nm $\leq$ 3.4ps/(nm·km)	
		1550nm $\leq$ 18 ps/(nm·km)	
		1625nm $\leq$ 22 ps/(nm·km)	
		Cutoff Wavelength $\leq$ 1260 nm	

		PMDQ (Quadrature average*) : ≤ 0.20 ps//km $^{1/2}$	
		MFD : 9.1 ± 0.4 μ m at 1310nm	
		MFD : 10.3 ± 0.5 μ m at 1550nm	
		Zero dispersion slope : ≤ 0.092 ps/(nm 2 ·km)	
		Zero dispersion wavelength : 1300~1324nm	
13	Temperature Range	Storage Temperature Range: -40°C to +75°C	
		Installation Temperature Range: -10°C to +60°C	
		Operating Temperature Range: -40°C to +75 °C	
14	Physical Properties	Complies to ANSI/TIA-568.3-D, ITU-T G652.D, Telcordia GR-20, IEC 60794-2, ISO/IEC 11801,ISO/IEC 24702	
		Cable Bend Radius : 20 x Cable Diam.	
		Cable Kink Radius : 10 x Cable Diam.	
		Cable Max. Tensile Strength (Short Term) : 2000 N	
		Cable Max. Crush Resistance (Short Term) : 3000 N / 100mm	
		Impact Resistance : 25 Nm	
15	Regulatory Compliances	OEM should be an ISO9001, ISO 14001 and ISO. The OEM shall be CE Certified. All Related documents to be submitted.	
16	RoHS Compliant	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	
17	Solution Compliance	All networking passive material (Fiber and Copper) should be from one OEM make only.	

22. 12F Core Multimode Fiber Optic Cable.

S. No.	Parameter	Specification	Compliance (Yes/No)
1	Product Code / Recommended Make	To be Specified by the Bidder	
2	Type	12F Core OM4 Multimode (50/125µm) Fiber optic Outdoor Cable	
3	Cable	12F Core Multi Mode Uniloose Tube, Single Sheath, Fiber cable is perfectly suited for both gigabit Ethernet and 10 gigabit Ethernet campus and backbone applications	
4	Application	Must be suitable for both 1 gigabit Ethernet and 10/25 gigabit Ethernet campus and backbone networking applications.	
5	Outer Sheath	UV Resistance HDPE Jacket / Black	
6	No. of Tube / Tube diameter	1 / 3.0 ± 0.1 mm	
7	Water Blocking Material	WS Tape	
8	Loose Tube Construction	Std. plywood reel: Uniloose Tube, Water Blocking with fibres. Individually colour coded optical fibres as per Global Standards	
9	Cable Specifications	Fiber Color / Fibers per Tube : Blue, Orange, Green, Brown, Grey, White, Red, Black, Yellow, Violet, Pink, Aqua Cable diameter : 9.0 ± 0.5 mm	
10	Optical Properties	Core Non-circularity : ≤ 6 %	
		Cladding Diameter : 125.0 ± 0.7 µm	
		Core/cladding Concentricity Error : ≤ 1.0µm	
		Cladding Non-circularity : ≤ 1.0 %	
		Primary Coating Diameter : 245±10µm	
		Coating/cladding Concentricity Error : ≤ 12µm	
		Attenuation Co-efficient	
		850 Wavelength (nm) : ≤2.5 dB/km	
		1300 Wavelength (nm) : ≤0.8 dB/km	
		Effective Modal Bandwidth : ≥ 4700MHz.km (OM4)	
		Attenuation inhomogeneity : ≤ 0.1dB(500)	
		Numerical Aperture : 0.275 ± 0.015	

13	Temperature Range	Storage Temperature Range: -40°C to +70°C	
		Installation Temperature Range: -10°C to +70°C	
		Operating Temperature Range: -40°C to +70 °C	
14	Physical Properties	Complies to ANSI/TIA-568.3-D, Telcordia GR-20, IEC 60794-2/60794-3-10, ISO/IEC 11801, ISO/IEC 24702	
		Cable Bend Radius : 20 x Cable Diam.	
		Cable Kink Radius : 10 x Cable Diam.	
		Cable Max. Tensile Strength (Short Term) : 3000 N	
		Cable Max. Crush Resistance (Short Term) : 3000 N / 100mm	
		Impact Resistance : 25 Nm	
15	RoHS Compliant	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	

23. UTP datapoint I/O box along with set of facelet, back box, keystone style cat6 modular jack

a) Face Plate

S. No.	Parameter	Specification	Compliance (Yes/No)
1	Make	To be Specified by the Bidder	
2	Type	UK Style with Built-in Dust Covers / Shutters	
3	Material	Fire-retardant Plastic, ABS + PC, White color, UK Style.	
4	Acceptability	Should be able to accept Cat6A, Cat6 and Cat5e information outlets, Modules, Keystone and Adaptors to suit all installation requirements	
5	Approvals	UL 94V-0	
6	No. of plates	2 Plates/Pieces Face Plate for better aesthetic look	
7	Mounting screws	Include mounting screws and Label Holders with Plastic covers	
8	Available	Single/Dual/Quad network faceplate	
9	Dimensions	(H x W x D) 86 x 86 x 14.42 mm	
10	RoHS Compliant	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	

b) Back Box for Face Plate

S. No.	Parameter	Specification	Compliance (Yes/No)
1	Make	To be Specified by the Bidder	
2	Type	Back Box for UK Style Faceplate	
3	Material	White High impact plastics.	
4	Entry	Adjustable cable entries	
5	Dimensions	38 x 87 x 87 mm	
6	Compatible	Back box allows for mounting a various ports of Faceplates	
7	RoHS Compliant	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	

c) Keystone Style Cat6 Modular Jack

S. No.	Parameter	Specifications	Compliance (Yes/No)
1	Make	To be Specified by the Bidder	
2	Type	CAT6 Modular Jack	
3	Type	Modular Jacks shall meet and exceed channel specification of ANSI/TIA 568.D-2, IEC/ISO 11801 & IEC 60603-7-41	

		when used as a component in a properly installed UTP channel.	
4	Housing Material	High impact Fire Proof ABS UL94V-0	
5	Front Connection	RJ 45 : PCB, 50 μ Phosphor bronze gold over nickel plating contacts	
6	IDC Connector	Phosphor bronze , Tin-plating contacts	
7	PCB Material & Thickness	FR-4, 1.2mm thickness	
8	Accessories	PCB Keystone Jack Can Be Easily Terminated by Hand Tool (Tool Should Terminate all 8 Pins in a Single Action) PCB based without soldering (solderless connectivity on PCB)	
9	Termination Interface	Front Mated Connection: 750 Cycles, Rear Mated Connection: 200 Cycles	
10	Plug and Outlet Contact force	≥ 100 Grams with FCC Compliant RJ-45 plug	
11	Plug retention Force	≥ 11 lbf	
12	Jack wire material and thickness	0.35mm Phosphor bronze gold over nickel plating	
13	IDC Conductor	0.5mm Phosphor bronze , Tin-plating	
14	Contact Compatibility	Accommodates 23 to 26AWG solid	
15	Termination Pattern	TIA / EIA 568 A and B	
16	Operating Temperature	-10° to +60°C	
17	Storage Temperature:	-40° to +70°C	
	Operating Humidity:	10% to 90% PH	
18	Electrical Performance	Insertion Loss: Max. 0.32 dB	
		NEXT: Min. 46.0 dB	
		FEXT: Min. 35.1 dB	
		RL: Min. 14 dB	
		PSANEXT: Min 56.5 dB	
		PSACRF: Min 53.0 dB	
		TCL: Min 20.0 dB	
		Insulation Resistance: $\geq 500\text{m}\Omega$	
		Contact Resistance: $\leq 10\text{m}\Omega$	
		Current rating: 1.5 Amps	
		DC Resistance: $\leq 0.1\Omega$	
		DC/AC Volt Endurance: DC1000V/AC750V 1min	
19	Regulatory Compliances	Should be ETL Verified for 04 Connector Channel and UL Listed	
20	RoHS Compliant	Should comply to RoHS Directive 2002/95/EC	

24. 1" PVC Pipe

S. No	Parameter	Specifications	Compliance (Yes/ No)
1	Nominal Diameter	Minimum 1 inch (25 mm)	
2	Material	Unplasticized PVC (uPVC)	
3	Pressure rating	Class B	
4	Wall thickness	Minimum 2.8 mm	
5	Application	Must be suitable for LAN cable conduit	
6	Standard	ASTM D1785/ ISO 1452	

25. 2" PVC Pipe

S. No	Parameter	Specifications	Compliance (Yes/ No)
1	Nominal Diameter	Minimum 2 inch (50 mm)	
2	Material	Unplasticized PVC (uPVC)	
3	Pressure rating	Class B	
4	Wall thickness	Minimum 3.9 mm	
5	Application	Must be suitable for LAN cable conduit and cable aggregation	
6	Standard	ASTM D1785/ ISO 1452	

26. Fluorescent warning tape

S. No	Parameter	Specifications	Compliance (Yes/ No)
1	Color	Fluorescent Red/Green/Orange/Yellow	
2	Material	Polyethylene	
3	Thickness	01-015 mm	
4	Width	100-150 mm	
5	Label Printing as	Caution- Network cable below	
6	Visibility	High visibility, UV resistant	
7	Tensile strength	Greater than 20 MPa	
8	Installation depth	1-1.5 feet below the ground	
9	Durability	Resistant to moisture, chemical and corrosion	

27. 2" CASING CAPPING MEDIUM SIZE

S. No	Parameter	Specifications	Compliance (Yes/ No)
1	Material of Construction	PVC with wall thickness of minimum 2mm	
2	Dimensions	width of 50 mm and Standard Length 2.5 Mtrs min.	
3	Manufacturing Standards	ISI marked	

28. 1" CASING CAPPING MEDIUM SIZE

S. No	Parameter	Specifications	Compliance (Yes/ No)
1	Material of Construction	PVC with wall thickness of min. 2mm	
2	Dimensions	Minimum of 25mm (W) x Standard Length 2/2.5 Mtrs	
3	Manufacturing Standards	ISI marked	

29. 40mm HDPE

S. No	Parameter	SPECIFICATIONS	Compliance (Yes/No)
1	Outer diameter	40mm	
2	Thickness	1.5 mm	
3	Co-efficient of friction	<0.5	
4	Blowing Pressure	up to 6 Bar	
5	Environmental stress crack resistance	As per TSM D-1693	
6	Manufacturing Standards	ISI Marked	
7	Certification	ISO Certified production facility	

30. 50mm GI pipe

S. No	Parameter	Specifications	Compliance (Yes/No)
1	Outer diameter	60 mm +/- 2 mm	
2	Wall Thickness	3 mm or more	
3	Coating	Hot dipped galvanised pipe with zinc coating thickness of 80 micron or above	
4	Resistance to rust and UV radiation	Pipe should have resistance to rust and UV radiation	
6	Manufacturing Standards	ISI Marked	
7	Certification	ISO Certified production facility	

31. ROUTE MARKERS

S. No	Parameter	Specifications	Compliance (Yes/No)
1	Type of construction	Pre-cast RCC/IRON	
2	Height of the Router Marker	at least 2.5 Feet.	
3	Width	at least 0.5 Feet	
4	Painted colour	All route markers shall be painted in blue/orange/yellow colour	
5	Height of each letter	at least 4 inches	

32. CABLE PULL PITS

S. No	Parameter	Specifications	Compliance (Yes/No)
1	Type of construction	Pre-cast RCC	
2	Diameter	30 inches or higher	
3	Depth	36 inches or more	
4	Chamber Cover	Heavy duty RCC slab	
5	Colour Code	Chamber shall be Red/Yellow painted with marking with each letter should be at least 4 inches	
6	Preferred Make	Locally fabricated with Sample testing and approval prior to supply	

33. Manhole chamber

S. No	Parameter	Specifications	Compliance (Yes/No)
1	Type of construction	Pre-cast RCC/ Concrete (M20) Manhole chamber	
2	Internal clear size	Minimum of 3 feet length and 2.5 feet width	
3	Depth	36 inches or more	
4	Wall thickness	Minimum 4 inches	
5	Base slab thickness	Minimum 6 inches	
6	Top cover slab thickness	Minimum 4 inches	
7	Manhole cover type	Precast RCC/ Cast Iron	
8	Cover opening size	Minimum 450 mm X 450 mm	
9	Colour Code	Chamber shall be Red/Yellow painted with marking with each letter should be at least 4 inches	
10	Number of duct entries	2 to 6 entries, located on opposite walls	
11	Duct/ cable entry	suitable for 40/50/63 mm HDPE conduits entry	
12	Duct sealing	Non shrink grout/ rubber grommets	

34.9 U Network Rack with accessories

Sl. No	Specifications	Compliance (Yes/No)
1	Racks manufactured out of steel sheet punched, formed, welded and Powder coated	
2	Rack should be from ISO 14001 ,27000 Certified Company & UL Listed	
3	Standard for Racks configuration will be welded frame with Integrated side panel and vented top cover	
4	Rack should have Front tinted Glass door	
5	Rack should have provision to mount racks on Wall	
6	Rack should be 9U in Height.	
7	It should be minimum 550MM Wide & 600MM Deep	
8	Rack should Conform to DIN 41494 or Equivalent EIA /ISO / EN/CEA Standard	
9	Rack should have Adjustable mounting depth,	
10	Rack should have 4 Nos. Adjustable, 19" verticals with Punched 10mm Square Hole and Universal 12.7mm-15.875mm-15.875mm alternating hole pattern offers greater mounting flexibility, maximizes usable mounting space.	
11	Rack should have Numbered U positions,	
12	Rack should have 100% assured compatibility with all equipment conforming to DIN 41494 (General industrial standard for equipment)	
13	Powder coated finish with seven Tanks pre-treatment process meeting IS	
14	Rack should have one Horizontal cable manager loop 1U.	
15	Rack should have one Cantilever shelf.	
16	Rack should have Fan module Mount Provision on top Cover with minimum 1 no. 90 CFM Fan	
17	Rack should have one Server /IT Rack mount power distribution unit, 1Ph, 230V, 8A, 50/60Hz, 2U standard with 6 X Indian Round Pin 5A, Inlet Plug type 6A Indian Round Pin, 8A Fuse - PDU Rating 1.8KVA/Side feed- 1.5Mt/ Black	
18	Rack should have provision for cable entry Exit from Both top & Bottom.	
19	Rack should have 1 Packet of mounting hardware, Pack of 20.	
20	Rack should have 24 Port 1U Angled Jack Panel Unloaded, Patch panels IDC (IDC of Information Outlet) Connectivity Snap in Type should be at rear end & RJ-45 jack on front panel, 19" rack mountable.	
22	Rack should have Straight Patch Panel with Angled Information Outlet Slot that makes patch cord routing easier and eliminate the need for Horizontal Cable Management.	
23	Patch Panel should be able to accept Cat6A, Cat6 and Cat5e information outlets for backward and forward compatibility	

35.27 U Network Rack with accessories

Sl. No	Specifications	Compliance (Yes/No)
1	Racks manufactured out of steel sheet punched, formed, welded and Powder coated	
2	Rack should be from ISO 14001 ,27000 Certified Company & UL Listed	
3	Standard for Racks configuration will be welded frame with Integrated side panel and vented top cover	
4	Rack should have Front tinted Glass door	
5	Rack should have provision to mount racks on Wall	
6	Rack should be 27 U(1U = 44.45 mm) in Height.	
7	It should be minimum 550MM Wide & 600MM Deep	
8	Rack should Conform to DIN 41494 or Equivalent EIA /ISO / EN/CEA Standard	
9	Rack should have Adjustable mounting depth,	
10	Rack 4 No Adjustable, 19" verticals with Punched 10mm Square Hole and Universal 12.7mm-15.875mm-15.875mm alternating hole pattern offers greater mounting flexibility, maximizes usable mounting space.	
11	Rack should have Numbered U positions,	
12	Rack should have 100% assured compatibility with all equipment conforming to DIN 41494 (General industrial standard for equipment)	
13	Powder coated finish with seven Tanks pre-treatment process meeting IS	
14	Rack should have one Horizontal cable manager loop 1U.	
15	Rack should have one Cantilever shelf.	
16	Rack should have Fan module Mount Provision on top Cover with minimum 2 no. 90 CFM Fan	
17	Rack should have one Server /IT Rack mount power distribution unit, 1Ph, 230V, 8A, 50/60Hz, 2U standard with 6 X Indian Round Pin 5A, Inlet Plug type 6A Indian Round Pin, 8A Fuse - PDU Rating 1.8KVA/Side feed-1.5Mt/ Black	
18	Rack should have provision for cable entry Exit from Both top & Bottom.	
19	Rack should have 1 Packet of mounting hardware, Pack of 20.	

36. 42U Network Rack

S. No.	Specifications	Compliance (Yes/no)
1	Rack manufactured out of steel sheet punched, formed, welded and Powder coated	
2	Standard for Rack configuration will be welded/CKD frame and side panels and vented top cover	
3	Rack should have Front Convex Single Perforated Door and Dual Perforated door at Rear.	
4	Rack should have 2 no's of removable side panel with slam latch.	
5	Rack should have provision to mount racks on Floor	
6	Rack should be 42U (1U = 44.45 mm) in Height.	
7	It should be 800MM Wide,1200MM Deep and Overall height 2115 MM.	
8	Rack should include adopter kit 1 no (loop type)	
9	Rack should Conform to DIN 41494 or Equivalent EIA /ISO / EN Standard	
10	Rack should have Adjustable mounting depth	
11	Rack 4 No Adjustable, 19" verticals with Punched 9mm Square Hole and Universal 12.7mm- 15.875mm-15.875mm alternating hole pattern offers greater mounting flexibility, maximizes usable mounting space.	
12	Rack should have Numbered U positions	
15	Powder coated finish with seven Tanks pretreatment process meeting IS	
16	Rack should have Proper Grounding & Bonding	
17	Rack should have Fan module Mount Provision on top Cover	

18	Rack should have Fan tray with 4 no's 90 CFM Fan	
19	Rack should have 1 No Fixed shelf with 715mm depth for mounting NON Rack mountable Equipments	
20	Rack should have 1 No Key Board shelf with 715mm depth	
21	Rack should have 2 Vertical and 2 Horizontal Cable manager	
22	Rack should have 2 No Server /IT Rack mount power distribution unit, 1Ph, 230V, 32A, 50/60Hz, Zero U standard with 12 X Indian Round Pin 5/15A, 16A MCB X 2 Circuits- PDU Rating 7.3KVA/Bottom feed-3Mt/ Black/ Inlet Plug Not Installed	
23	Rack should have provision for cable entry Exit from Both top & Bottom.	
24	Rack should have 1 Packet of mounting hardware, Pack of 20.	

37. 5 KVA online UPS along with batteries

S.No	Parameter	Specification	Compliance (Yes/No)
1	Power rating	5 KVA or higher	
2	Input	Voltage: 220-240V Single Phase AC Frequency range: 48-52 Hz Phase: Single Phase with ground Power factor: >0.8	
3	Output	Voltage: 230V +/- 1% Single Phase AC Voltage regulation: +/- 1% Frequency: 50 Hz Output waveform: Pure sinewave Efficiency: >90% Crest factor: 3:1 Power factor: 0.8-0.9 THD: Maximum 2% at 100% linear load.	
4	Battery	Battery type: SMF VLRA stationary lead acid batteries conforming to JISC : 8702 (Pt I,II & III) Batteries current rating should be chose to provide 180 minutes backup at full load.	
5	Switching technology	IGBT-PWM	
6	Design	UPS should have in-built isolation transformer with rated power, ON/OFF MCB for Input, ON/OFF MCB for output and ON/OFF MCB for Battery DC Voltage. Should have IP20 rated enclosures.	
7	Protection	Protection for under voltage at battery terminal, over voltage protection, short circuit and over load protection at UPS output terminal. Over temperature protection.	
8	Overload limit	20% over load for 5 minutes	
9	Backup Time	Minimum 180 min at full load.	
10	Metering	Input voltage, output voltage, input frequency, output frequency. DC Voltage, DC Charging Current, AC Output current.	
11	Alarms & Indicators	Mains on/off, Load level, battery level, battery charging and discharging. over load. Battery low voltage with audible alarm, Over load with audible alarm, over temperature with audible alarm.	
12	Installation	Included in the scope of supply	
13	Management features	The UPS should include a 10/100/1000 Ethernet port and support SNMP. The UPS health status should be monitored over the network.	
14	Certifications	BIS, ROHS	
15	Accessories	The scope of supply should include a battery rack, copper power cables with the appropriate current	

		rating, and sufficient length to position the battery bank 5 meters away from the UPS. Additionally, cables should be provided to connect the UPS to the Mains Distribution, which is also located 5 meters away.	
16	Warranty	3 years or more onsite comprehensive OEM warranty	

38.1 KVA online UPS along with batteries

S.No	Parameter	Specification	Compliance (Yes/No)
1	Input	Voltage: 220-240V Single Phase AC Frequency range: 48-52 Hz Phase: Single Phase with ground Power factor: >0.9	
2	Output	Voltage: 220V +/- 1% Single Phase AC Voltage regulation: +/- 1% Frequency: 50 Hz Output waveform: Pure sinewave Efficiency: >90% Crest factor: 3:1 Power factor: 0.8-0.9 THD: Maximum 3% at 100% linear load.	
3.	Battery	Battery type: Sealed lead maintenance free, lead acid tubular. Batteries should be placed inside the UPS enclosure.	
4.	Switching technology	IGBT-PWM	
5.	Protection	Protection for under voltage at battery terminal, over voltage protection, short circuit and over load protection at UPS output terminal. Over temperature protection.	
6.	Backup Time	Minimum 60 min at full load.	
7.	Metering	Input voltage, output voltage, input frequency, output frequency.	
8.	Indicators	Mains on/off, Load level, battery level	
9.	Installation	Included in the scope of supply	
10	Certifications	BIS, ROHS	
11	Warranty	Minimum 3 years for UPS and Batteries	

39. POWER CABLING FOR UPS IN & OUT

S. No	Parameter	Specifications	Compliance (Yes/ No)
1	Insulation material	XLPE (cross linked polyethylene)	
2	Sheath material	FRLS (Flame retardant low smoke)	
3	Conductor material	Annealed electrolytic Copper	
4	Conductor size	2.5 sq mm minimum	
5	Current carrying capacity	≥ 18 amps	
6	Insulation resistance	$\geq 1000 \text{ M}\Omega\text{-Km}$	
7	Maximum Conductor temperature	90 deg C or more	
8	Certification	IEC 60228, IS 7098	
9	Voltage grade	1100 V	
10	Marking	Manufacturer name, size, voltage grade, FRLS marking	
11	Packing	Coils/ Drum with protective warping	

Scope of Supply

The scope of this procurement includes the supply, installation, and configuration commissioning of Camus network infrastructure at DMRL and ATC. Bidder has to supply the following products/items as per the technical specifications outlined in Annexure-I at DMRL Kanchan Bagh and ATC Devatalagutta, Hyderabad. Bidder has to perform the installation and commissioning as mentioned.

S. No	Description of Items	UoM	DMRL	ATC	Total
A	Active Network Components				
1	24 port Core switch	Nos	4	2	6
2	24 port Distribution Switch	Nos	8	0	8
3	48 port Managed Access Switch	Nos	8	0	8
4	24 port Managed Access switch	Nos	58	10	68
5	12 port Managed Access switch	Nos	58	12	70
6	10G Single Mode SFP transceiver module	Nos	40	4	44
7	10G Multi Mode SFP transceiver Module	Nos	132	24	156
8	1G Single Mode SFP transceiver module	Nos	14	2	16
9	1G Multi Mode SFP transceiver Module	Nos	92	14	106
10	Next Generation Firewall	Nos	1	1	2
11	Network Access Control appliance	Nos	1	-	1
12	Network Access Control licence	Nos	800	-	800
13	Software Defined Network (SDN) controller appliance	Nos	1	-	1
14	86" Display for Network Monitoring	Nos	4	0	4
B	Passive network components				
15	Cat 6 UTP Cable (305 Meter roll box)	Nos	160	20	180
16	Cat6 Unshielded LSZH Patch Cords with 1 meter length	Nos	1000	100	1100
17	Cat6 Unshielded LSZH Patch Cords with 2-meter length	Nos	1000	100	1100
18	12F 1U Rack Mount Fiber Enclosure (LIU) including Splice Trays, Pigtails, and Couplers	Nos	60	12	72

19	48F Rack Mount Fiber Enclosure (LIU) including Splice Trays, Pigtails, and Couplers	Nos	34	4	38
20	LC-LC Duplex Single mode Fiber Patch Cord	Nos	70	30	100
21	LC-LC Duplex Multi-mode Fiber Patch Cord	Nos	250	-	250
22	12F Core Single mode Fiber Optic Cable.	mtrs	6500	2200	8700
23	12F Core Multi mode Fiber Optic Cable.	mtrs	9500	2000	11500
24	UTP Datapoints I/O Box along with set of faceplates, back box, Keystone Style Cat6 Modular Jack	Nos	1000	100	1100
25	1" PVC pipe	Mtrs	4500	500	5000
26	2" PVC pipe	Mtrs	250	74	324
27	Fluorescent warning tape	Mtrs	8500	2500	11000
28	2" Casing capping medium size	Mtrs	1000	167	1167
29	1" Casing capping medium size	Mtrs	5000	238	5238
30	40mm HDPE conduit pipe	Mtrs	15000	4000	19000
31	50 mm GI pipe	Mtrs	500	180	680
32	Route Markers	Nos	300	100	400
33	Cable pull pits	Nos	50	6	56
34	Manhole chambers	Nos	70	10	70
C	Rack Enclosure & Power Backup Management				
35	9U Network Rack with accessories	Nos	58	8	66
36	27U Network Rack with accessories	Nos	4	0	4
37	42U Network Rack with accessories	Nos	3	1	4
38	5 kVA online UPS along with batteries	Nos	4	1	5
39	1 kVA online UPS along with batteries	Nos	60	6	66
40	Power Cabling for UPS In & Out	Mtrs	1000	0	1000

Installation & Configuration

For the successful implementation of the Installation and commissioning of campus network infrastructure, the Bidder is responsible for the following tasks at both DMRL and ATC.

Part-A: Installation and commissioning of campus network infrastructure at DMRL

- I. Passive network cabling: Laying of OFC and Installation of passive network cables, network enclosures and accessories.
- II. Active network components installation:
 - a) Installation and configuration of network switches.
 - b) Installation and configuration of firewalls
 - c) Installation and configuration of the Network Access Control & Software Defined Networking.

- d) Implement the Network Monitoring System (NMS) for centralized network monitoring and control.
- III. Installation of UPS for access and distribution network switches
- IV. Integration of DMRL and ATC networks to monitor and manage ATC network devices from DMRL.

Part B: Installation and commissioning of campus network infrastructure at ATC.

- I. Laying of OFC cable for expanding the connectivity to all the building locations
- II. Laying of UTP cable for additional network I/O points
- III. Installation and configuration of network switches, firewall and UPS.

Part C: Training & Documentation

Part D: Onsite support for Operations, troubleshooting and management

Installation and commissioning of campus network infrastructure at DMRL

I) Passive network Cabling:

1. Bidder should submit network evaluation plan, Architecture and relevant information for establishing two parallel networks one for intranet and one for internet at DMRL and its other campus.
2. Under this scope, Bidder is also responsible for establishing the physical network cable connectivity among the switches, servers, computers and network printers for network connectivity through Intranet LAN and Internet LAN.
3. Bidder is responsible for 10000 meters of Trenching, HDPE laying & FO cabling with backfilling and 900 meters of Road cutting, trenching and re-cementing at DMRL.
4. Bidder should prepare the OFC network layout and submit to the DMRL. Network layout plan, to be approved by DMRL before initializing the passive network cabling activity.
5. The bidder shall ensure that all fiber optic cabling and UTP cabling works are designed, installed, tested, and documented in full compliance with the applicable ISO/IEC standards, including but not limited to ISO/IEC 11801, ISO/IEC 14763 (Parts 1-3), ISO/IEC 61935-1, ISO/IEC 60793/60794, ISO/IEC 61156, and ISO/IEC 30129.
6. Any materials, installation practices, testing procedures, and certification results not conforming to the above-mentioned standards shall be deemed non-compliant, and the bidder shall rectify such deficiencies at no additional cost to the DMRL.
7. Bidder should establish the physical fiber cable connectivity in redundancy to all the distribution switches from core switches. Each distribution switch should be physically connected to two different core switches configured in HA and fiber line should be active in both uplinks.
8. It involves the laying of fiber optic cable, fiber splicing (SM/MM), and terminating fiber cable with LIUs at network switch racks. Bidder should provide the necessary material to interface the fiber at network racks.
9. Fiber optic cable laying involves digging of the trench of depth 3 feet and 1.5 feet width on the ground throughout the required length for fiber cable laying. The fiber cable should be laid through standard HDPE conduit of ISI mark as per outlined technical specifications. The trench is to be filled with sand and gravel and these cables shall be terminated at LIUs.

10. Bidder shall dig the road, if necessary, the road cutting of size 1ft X 1.5ft (deep) for laying of UG Cable through the standard GI conduit of ISI Mark pipe and road is closed with cement and gravel.
11. Bidder should carry out the laying of UTP cable for network connectivity to about 1000 nodes in both networks at DMRL. Bidder should use cat6 UTP cable with different colour for Intranet and Internet connections. The UTP cable should be laid through PVC pipes while routing through fall ceiling or walls.
12. The Bidder should be responsible for installing network racks for the core and distribution switches on the floor. Additionally, all access switch network racks should be wall-mounted in the corridors of all buildings at a height of at least 8 feet, and should be below the ceiling.
13. Bidder is required to arrange the cables neatly and affix identification tags on each cable at network switch. Bidder should terminate the UTP cable at I/O box with identification tags. The Bidder should provide required material at no additional cost.
14. Bidder should install the cat6 jacks at each network switch rack and terminate the UTP cable at jacks.
15. Construct cable pulling pits at intervals as required for ease of fiber optic cable laying and maintenance, typically every 200–250 meters, or as specified in the fiber route plan. All pull pits must be constructed as per ISO/IEC 14763-2 or relevant industry standard.
16. Pull pits shall be made of precast concrete slabs or brick masonry, depending on site conditions and approvals. Ensure pull pits are having minimum internal dimensions: 600mm x 600mm x 600mm equipped with concrete covers (minimum 5-ton load bearing) for durability and safety and properly aligned and levelled with the ground to prevent tripping hazards.
17. Pull pits should include entry/exit conduits for fiber duct/cable and drainage arrangement (if applicable) to avoid water stagnation
18. Install route markers along the entire fiber path at intervals of 50 meters, and at all bends, joints, road crossings, and significant landmarks. Route markers must be made of durable material (e.g., concrete, GI plate, or UV-stabilized plastic), weatherproof and tamper-resistant. Markers should be painted or color-coded for visibility. Route markers samples may be tested and approved prior to supply
19. Construct fiber cable manholes at key locations (e.g., junctions, building entry points, bends exceeding 45°, long straight stretches over 300m). Manholes shall be made using either Standard brick masonry (9" thick walls) with plastering and waterproofing OR Precast reinforced concrete (RCC) or HDPE/Fabric modular manholes (subject to approval)
20. Manhole should have minimum internal dimensions as Standard manhole: 1000mm x 1000mm x 1000mm or large manhole (if required): 1200mm x 1200mm x 1200mm
21. Manhole should be covered with heavy-duty RCC or Cast-Iron cover, load rating of at least 10 tons. And manholes must include entry sleeves or conduit inlets, Proper cable racking and support brackets, Drainage arrangements (sump or gravel bottom) and labelling for cable identification
22. All civil works must be executed as per the approved fiber route design.
23. All trenches and pits must be backfilled and restored to original condition post-installation.
24. All tasks must be carried out under supervision of the DMRL representative and be subject to inspection and approval.

25. All the required cables, accessories, manpower and any other additional hardware not mentioned in the scope of supply for the installation are in the scope of bidder. Remaining material after completion of Job has to be handed over to DMRL.
26. It is also the bidder responsibility to handover the installation area neat and orderly after the installation of the system.
27. It is also the bidder responsibility to ensure that there is no disturbance or damage to the other existing network cables, power cables and telephone cables. Bidder is responsible for restoring the cable connectivity if there is any damage.
28. Bidder should attend the pre-bid meeting for detailed layout of network.

II) Active network components installation:

a) Installation and Configuration of network switches

29. Bidder should install all the core, distribution and access switches at network racks.
30. Bidder should configure initial settings for the devices to establish the basic network parameters. Implement essential configurations on switches for proper operation.
31. Bidder should Setup high availability features to ensure redundancy and failover capabilities. Verify proper functioning of high availability configuration through rigorous testing.
32. Configure redundant Core Switches in the Active-Active mode in order to achieve the higher switching and backplane capability
33. Air gapped network should be built with maximum redundancy as per solution requirement
34. Network should be free of Spanning Tree and employ Layer-3 at access level.
35. All the switches proposed must support Layer-3 dynamic routing protocols and must be compatible with the NAC solution.
36. All the Core switches shall facilitate high capacity, non-blocking switching with installed redundant power supplies and fans from Day 1 in order to achieve higher performance with network resiliency.
37. The proposed solution should be scalable for future upgrades to higher speed network operations and expansion
38. Bidder should Setup strong passwords and essential security features for network protection.
39. Bidder should setup VLAN Trunking Protocol (VTP) domain to manage VLANs effectively.
40. Bidder should configure management access for switches to allow authorized users.
41. Bidder should create VLAN Configurations & Segmentation: Design and implement VLAN configurations for network segmentation. Assign VLANs to interfaces for proper traffic management. Provide descriptions for interfaces to aid in network administration.
42. Setup port channels for link aggregation.
43. Implement and fine-tune Spanning Tree Protocol for network loop prevention.
44. Configure routing to enable segmentation of network traffic. Setup routing policies to optimize data flow.
45. Configure SNMP and syslog for network monitoring and logging. Setup performance measurement and monitoring mechanisms.
46. Bidder should Configure Topology-Independent Loop-Free Alternate (TI-LFA): Implement TI-LFA for fast rerouting in case of link failures.
47. The Bidder should integrate identity services with Active Directory (AD) if available. If AD is not available, the Bidder must create a new identity service for user authentication.

48. Bidder should configure access control lists for security policies.
49. Bidder should configure Uplink & Downlink Switch port.
50. Bidder should integrate the network devices with branches, WAN, and LAN segments.
51. Bidder should configure switches for security & performance enhancement, configure for traffic isolation, MAC filtering, port security, VLANs, QoS, and link aggregation.
52. Bidder should shut down unused ports, disable unused switch ports for improved security.
53. Configure the switches for user-based access. All the switches should be configured for two accounts. One is administration account with full access privileges and User account with limited access.
54. Bidder should supply and configure the TFTP server to regularly backup the configurations and update the OS patches of network switches. Configure the switches accordingly.
55. Bidder is responsible for the provision of network switches patch/OS updates during the warranty period.

b) Installation and configuration of NGFW

56. Install the NGFW hardware in a suitable rack or chassis. Securely mount the firewall in the rack or place it in an appropriate physical location. Connect the necessary network cables to the relevant ports (WAN, LAN, DMZ).
57. Perform testing to verify connectivity between LAN, WAN and DMZ.
58. Assign a static IP address to the management interface. Set up initial system settings, including hostname, time zone, and admin credentials.
59. Providing appropriate licensing keys for NGFW features (e.g., VPN, IPS, URL filtering,). Validate license activation and ensure all licensed features are accessible.
60. Configure NAT rules to enable private IP addresses to communicate with external networks. Set up appropriate source and destination NAT for outbound and inbound traffic, as per DMRL requirement respectively.
61. Define security policies to allow or deny traffic between different zones.
62. Create rule-based policies for allowing web traffic, email traffic, VPN connections, and more.
63. Set up specific security rules for applications, ports, and protocols.
64. Configure application-aware filtering if required.
65. Configure IPS policies to monitor and block known threats or suspicious activity. Customize IPS rules according to the network environment and threat landscape.
66. Enable logging of security events, traffic logs, and system events.
67. Configure a syslog server or integrate with a Security Information and Event Management (SIEM) system for centralized logging and analysis. If a SIEM system is not available, the bidder must provide an alternative solution for effective log collection and analysis.
68. Configure alerts for specific security incidents or system anomalies.
69. Enable real-time antivirus and anti-malware scanning for network traffic.
70. Setup file inspection policies for HTTP, FTP, and other protocols.
71. Setup URL filtering to block access to malicious websites or anomalies sites.
72. Create categories of allowed and blocked websites based on DMRL requirement.
73. Create and integrate with a directory service (Active Directory/ LDAP) for user authentication and identity mapping.
74. Configure user-based access controls and policies.

75. Configure the firewall to block or unblock the services for all the network-connected clients from the server.
76. Create a dashboard template to monitor all the features of firewall, and integrate with monitoring displays.

c) Installation of Network Access Control:

77. Bidder should configure hardware resources and network device configurations to ensure compatibility with Network Access control (NAC). NAC to be installed on designated hardware as per specifications mentioned in annexure –I.
78. Security certificates are to be implemented to ensure a secure network environment.
79. Initial network access policies are established to control user and device access in the both the networks.
80. The Bidder should integrate NAC with routers, switches, and other network devices in the LAN.
81. RADIUS and TACACS+ settings are configured on the network devices for seamless communication with NAC.
82. Bidder should create Authentication, Authorization, and Accounting (AAA) policies to manage access in the both LANs. Controlled access tests are to be performed to validate communication between the LAN devices and NAC.
83. Bidder should setup NAC dashboard to provide real-time monitoring of the network health and security of Intranet and Internet Networks. Monitoring tools and alert systems are to be deployed to track the performance and security of the networks.
84. A final validation is to be conducted to ensure that the NAC system is fully operational within the new LANs.
85. The Bidder should provide training to the DMRL IT team on managing and maintaining NAC.

d) Implementing Network Monitoring System (NMS):

86. Bidder should supply and install the Network monitoring and management system.
87. Configure routers, switches, firewalls and existing server infrastructure to link the NMS with the network (Intranet and Internet). Install and configure servers to host monitoring tools, databases, and incident management systems.
88. The Bidder should provide, deploy, and configure network monitoring and management tools that integrate network monitoring, device management, and device configuration capabilities to track network performance, configure devices, detect anomalies, and generate alerts. Bidder should provide all the required licenses at no additional cost.
89. Bidder should configure the NMS dashboard to display real-time data of network health, traffic, and alerts. All these features should be displayed on monitoring display.
90. Bidder should setup user roles, permissions, and access control policies to ensure only authorized personnel can access NMS systems.
91. Bidder should configure firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) to secure NMS communications.
92. Bidder should ensure all NMS communications, especially remote access (if required any), are encrypted using VPNs or other secure protocols.
93. Bidder should test all NMS components, including hardware, software, and network connectivity, to ensure they function as expected. In addition, demonstrate the monitoring of network traffic and performance to validate that the NMS is capturing and analysing data accurately.

94. Conduct simulated network incidents to test the NMS's response mechanisms, including alerting, incident management, and resolution processes.
95. Perform vulnerability assessments and penetration testing to ensure the NMS's security measures are effective.
96. There should not be any subscription-based license policy, bidder should provide all the required licenses with life time validity.

III) Installation of UPS

97. The bidder shall supply and install the Uninterruptible Power Supply (UPS) systems. The UPS systems shall be used to provide uninterrupted power to all network switches installed at different buildings.
98. The UPS shall be securely mounted using appropriate rack rails or mounting kits. Proper ventilation and clearance shall be maintained as per manufacturer recommendations. The bidder shall connect each UPS to the respective network switch or group of switches as per the approved design.
99. DMRL will provide the utility electrical power supply port within 5 meters from the access switch network racks. It is bidder responsibility to provide electrical wiring to the UPS and network rack PDU. Power cabling shall be neatly routed and properly labelled.

IV) Integration of DMRL and ATC networks

100. The DMRL and ATC campus are located approximately 10 km apart and are not connected via direct fiber. Both campuses are connected through a WAN link. The bidder shall configure Network Access Control (NAC), firewalls and the Network Management System (NMS) to enable monitoring and management of the ATC campus network infrastructure from the DMRL network centre.

Installation of network infrastructure at ATC

I) Expanding the fiber cable connectivity

101. Under this scope of work, the Bidder shall also be responsible for expansion of fiber optic cable connectivity at the branch office, extending from the core switch location to all building locations that currently do not have network connectivity within the existing network infrastructure.
102. The fiber optic cable laying and related works at the ATC shall be executed in accordance with the same procedures, standards, and practices adopted for fiber laying at the DMRL. It involves the laying of fiber optic cable, fiber splicing (SM/MM), and terminating fiber cable with LIUs at network switch racks. Bidder should provide the necessary material to interface the fiber at network racks.
103. Bidder is responsible for 3000 meters of Trenching, HDPE laying & FO cabling with backfilling and 100 meters of Road cutting, trenching and re-cementing at ATC.
104. The Bidder should be responsible for installing network racks for the core switches on the floor. Additionally, all access switch network racks should be wall-mounted in the corridors of all buildings at a height of at least 8 feet, and should be below the ceiling.

II) Laying of UTP cable for additional network I/O points

105. Bidder should carry out the laying of UTP cable for network connectivity to about 100 nodes in both networks at ATC. Bidder should use cat6 UTP cable with different color for

Intranet and Internet connections. The UTP cable should be laid through PVC pipes while routing through fall ceiling or walls.

106. Bidder is required to arrange the cables neatly and affix identification tags on each cable at network switch. Bidder should terminate the UTP cable at I/O box with identification tags. Bidder should install the cat6 jacks at each network switch rack and terminate the UTP cable at jacks. The Bidder should provide the required material at no additional cost.
107. The UTP cable laying and related works at the ATC shall be executed in accordance with the same procedures, standards, and practices adopted for UTP cable laying at the DMRL.

III) Supply and installation of network switches, firewall and UPS

108. Bidder should replace the outdated core and access switches with latest model switches as per technical specifications and install in designated network racks. Additionally, bidder is responsible for supply and installation of additional network switches at new buildings to provide the network connectivity.
109. Bidder should configure initial settings for the devices to establish the basic network parameters. Implement essential configurations on switches for proper operation.
110. Supply and install the NGFW hardware in a suitable rack. Securely mount the firewall in the rack or place it in an appropriate physical location. Connect the necessary network cables to the relevant ports (WAN, LAN, DMZ).
111. Perform testing to verify connectivity between LAN, WAN and DMZ.
112. Assign a static IP address to the management interface. Set up initial system settings, including hostname, time zone, and admin credentials.
113. Supply and install the UPS systems for all network switches.
114. The installation and configuration of network switches, firewall and UPS systems shall be executed in accordance with the same procedures, standards, and practices as per Part-A.

Part C: Training and Documentation

115. **Training:** After successful completion of implementation. The Bidder should provide the training to the IT staff of DMRL for 5 working days on
 - a) Network switches performance monitoring and troubleshooting.
 - b) Network switches configuration backup, restore and firmware upgrades.
 - c) Creating and managing security policies, NAT rules, application policies, URL filtering in firewall.
 - d) Configuring and tuning IDS/IPS policies.
 - e) Creating user based/role-based policies.
 - f) Using dashboards for real time traffic monitoring and report generation.
 - g) Operational management of network access control and Software defined LAN.
116. **Documentation:** The Bidder should provide the documentation for the following
 - a) Bidder should provide the complete solution document including the fiber optic cable layout, network architecture, Network racks positioning, switches configuration, firewall configuration, NMS configuration, end point IP details along with the port number of switch to which it was connected. It should also include the troubleshooting steps for the entire solution. Bidder should provide the two documents in colour on 100 GSM paper binding.

- b) Bidder should provide the eco solvent flex of fiber optic cable layout of DMRL and ATC along with building locations.
- c) Standard operating procedures for the entire network infrastructure operation and maintenance should be provided in documents.

Part D: Onsite support for operations, troubleshooting and management of network infrastructure

117. Upon successful completion of installation and commissioning, the Bidder shall deploy qualified service engineers for on-site assistance for operations, troubleshooting and management for the complete network infrastructure including backbone fiber cabling, UTP cabling and UPS systems implemented under this tender for 3 years from the effective date of final acceptance.
118. It is the bidder responsibility to maintain the network available for 24/7 hours.
119. Bidder should deploy resident service engineers to maintain the network infrastructure during 8.40 Hrs to 17.10 Hrs on all working days.
120. If there is any discontinuity due to damaged network cable, Bidder resident service personnel should restore the physical network cable connectivity by performing the laying of new UTP cable or splicing of the fiber cables, the material required for restoring the cable connectivity is in bidder scope
121. The deployment shall include L3 Service Engineer, L2 Service Engineer and L1 Service Engineer. Each engineer must possess prior experience and qualifications corresponding to their designated level.
122. The roles are classified into three levels (L3, L2, and L1), each with increasing responsibilities and expertise as follows

S.No	Service engineer expertise	Responsibilities
1	Level 3 Engineer	1) Resolve complex network problems, including performance bottlenecks, security incidents, and multi-vendor interoperability issues. 2) Oversee critical network incidents and outages, ensuring swift resolution and minimal downtime. 3) Manage advanced network monitoring systems to track performance, identify potential issues, and ensure reliability. 4) Update firmware and patches of all the network components as per OEM and DMRL approval. Bidder should provide the firmware and patch updates. 5) Provide service as expertise in Layer 3 protocols (BGP, OSPF, EIGRP), MPLS, and SD-WAN. 6) Assist IT team in troubleshooting issues that require in-depth knowledge of firewall technologies, VPNs, and network security protocols. 7) Setup alerting mechanisms for hardware failures, high utilization, and security threats.

		8) Monitor and maintain firewall policies and IPS/IDS signatures. 9) Perform monthly vulnerability scanning of network devices and servers. Review logs and provide monthly security summary reports. 10) Ensure that the maximum cumulative downtime for both Networks in a year should not exceed 10 working days in case any hardware failure occur. 11) Provide quarterly capacity planning reports with recommendations.
2	Level 2 Engineer	1) Perform quarterly preventive maintenance for network infrastructure. Clean, inspect, and verify proper operation of network switches, firewall, SDN, NMS, NAC system and UPS systems. 2) Regularly analyse system performance (CPU, memory, storage, network) of network switches and servers. 3) Ensure the end-to-end network connectivity. 4) Any complaints (other than hardware failures) should be attended within 2 hours from the period of logging the complaints 5) Work with other IT teams, including security and systems administrators, to ensure seamless integration of network services. 6) Validate configuration consistency and compliance with best practices. 7) Ensure that detailed documentation of configurations, topologies, and incident resolutions are maintained. 8) Perform monthly vulnerability scanning of network devices and servers. Review logs and provide monthly security summary reports 9) Maintain updated configuration backups for all devices. 10) Apply configuration changes upon request and per schedule. 11) Provide monthly reports on network availability
3	Level 1 Engineer	1) Respond and resolve the hardware/software faults within the stipulated time. 2) Replace faulty components under warranty/support agreement. Troubleshoot and resolve network outages and performance issues. 3) Any complaints (other than hardware failures) should be attended within 2 hours from the period of logging the complaints 4) Work with other IT teams, including security and systems administrators, to ensure seamless network connectivity. 5) Regularly monitor the health of UPS systems installed for network switches. 6) Ensure the end-to-end network connectivity.

123. In the event of non-compliance, poor performance, or unsatisfactory service by any deployed engineer, the Bidder shall promptly replace the engineer with a suitably qualified expert within 3 days.

ACCEPTANCE CRITERIA

1. All network components must operate according to the specifications outlined in the Annexure-I.
2. All the services email, web, database, proxy, DNS, NTP, LDAP and Active directory must be operational and accessible after the successful commissioning.
3. Any technical issues identified during testing must be resolved before final acceptance.
4. All security measures and protocols, including access controls, and vulnerability protection must be properly implemented and tested. No critical security vulnerabilities should be present.
5. The implementation must comply with all relevant industry standards and regulatory requirements.
6. All configuration and setup documentation must be complete and accurate. Test reports and issue logs should be comprehensive and available for review.
7. The complete solution is accepted only after the completion of acceptance test as follows:

A) Access Switches Acceptance Test

- a. **Configuration Verification:** VLAN configuration matches design, Port security enabled (MAC binding, sticky MAC if needed), Management IP reachable via ping, SNMP configured and responding.
- b. **Performance:** Power-on self-tests (POST) pass, uplink to distribution switch is active and correct speed/duplex, Speed and duplex settings correct on all ports, Latency check, minimum 50 MBps (megabytes per second) upload/download speed at client in intranet.

B) Distribution Switches Acceptance Test:

- a. **Performance:** Power-on self-tests (POST) pass, uplink to core switch is active and correct speed/duplex, Speed and duplex settings correct on all ports, Latency check.

- b. **Redundancy & Routing:** Redundant uplinks to core switches function correctly, HSRP/VRRP configured and failover tested, Routing protocol (OSPF/EIGRP/Static) configured and working, Inter-VLAN routing working as designed.
- c. **Security & Management:** Access Control Lists (ACLs) applied as per design, SSH access with key or TACACS+/RADIUS authentication, Loop prevention protocols active.

C) Core Switches Acceptance Test

- a. High Availability & Redundancy: Dual core switches configured with redundancy (VSS, Stack, MLAG, etc.), Failover test between core switches, Routing table consistent with design.
- b. Routing and Performance: BGP/OSPF/Static routes verified, high-speed interfaces (10G/40G) are operational, perform end-to-end latency test and report the latency.
- c. Security & Monitoring: Control plane policing (CoPP) enabled, Secure management access (SSH, AAA), NetFlow/sFlow enabled (if required).

D) Firewall acceptance test

- a. Firmware/software is latest and approved
- b. Interfaces configured with correct IPs and zones
- c. Test deny rules for unwanted traffic
- d. IPS/IDS is enabled on correct interfaces/zones
- e. Generate test intrusion attempts to validate detection
- f. Monitor logs for accurate alerting (no false positives)

E) Other general tests (for all devices)

- a. Physical installation is complete (racking, grounding, power)
- b. Confirm cabling is labeled and neat
- c. Verify power-on self-tests (POST) pass
- d. Ensure console/SSH access is possible
- e. Check firmware/software version compliance with standards
- f. Ensure redundant network connectivity between core and distribution switches.
- g. Failover mechanisms must successfully handle simulated failures without service interruption.
- h. Licensing requirements for software and services must be met.

- F) Network Bandwidth Test:** Latency, bandwidth, and jitter of the entire network should be measured as per RFC 2544 and ITU-T Y 1564 standards for minimum 60 minutes and it should be within acceptable limits as follows.

S.No	Testing parameter	Acceptable limits
1	Access port throughput	≥ 900 Mbps
2	Access switch uplink throughput	$\geq 80\%$ utilization under load
3	Core to distribution bandwidth	≥ 9.5 Gbps
4	Packet loss	$< 0.1\%$ at max load
5	Average Latency	< 2 ms
6	Jitter	< 1 ms
7	Average download or upload data transfer speed for any end point in intranet.	≥ 50 MBps (Megabytes per second)

The software or hardware tools required to conduct the acceptance test are in the scope of supplier.

Bidder Qualification Criteria

1. The supply, installation and commissioning of campus network infrastructure requires a precise planning and site-specific customisation to ensure seamless installation, integration and performance of the supplied products and associated infrastructure. So, prior to the submission of bid, the bidder should visit the DMRL for the Pre-bid meeting. After the pre bid meeting a report of discussions carried out during the pre-bid meeting will be issued by DMRL. Attending the onsite Pre-bid meeting is mandatory. The bidder has to attach the record of discussions along with the technical bid.
2. All bidders shall submit a duly signed Confidential Non-Disclosure Agreement (CNDA) in the prescribed format mentioned in Annexure-VI as part of the bidding process. Submission of the CNDA is a prerequisite for participating in the pre-bid conference.
3. Bidder should be an Authorized seller/dealer/partner/distributor of the OEM for Network Switches, SFP transceiver modules, Next Generation Firewall, Network Access Control appliance, Optical Fiber Cable and UTP cables. Signed Manufacturer Authorization letter from the OEMs mentioning the bid number should be submitted along with the technical bid.
4. Bidder should have experience in supply, installation and configuration of more than 20 Nos of network switches and laying of more than 5 km OFC cable network in a single tender at any Government or Public Sector Undertaking organizations. Copies of the minimum 2 supply orders of the same (not older than 5 years from the bid opening date) and user acceptance reports has to be submitted along with the technical bid.
5. Bidder should have registered office/ branch office at Hyderabad/ Secunderabad region with adequate CCIE and CCNP certified engineers in their payroll. The registration certificate with office address and the details of the staff with their technical skills has to be submitted along with the technical bid.
6. Bidder should submit supporting documents including technical data sheet from OEM for all the offered products.
7. Bidder should have ISO/IEC 20000-1:2018 and ISO 9001:2015 certifications.
8. During the warranty period, on-site technical assistance is to be provided by the

bidder/OEM or authorized technical experts within 24 Hrs, if there is any hardware issue. The bidder should submit an undertaking in this regard.

9. The Firm should not be blacklisted in last 5 years by Central Government/State Govt., Public or Private Sector Enterprises. The bidder should submit an undertaking in this regard.
10. Bidder should provide the malicious code free design certificate from the OEM for the offered Network Switches, Next Generation Firewall and Network Access Control appliance.

TERMS & CONDITIONS

1. All the Network switches and SFP modules should be from same OEM.
2. All the Cat6 UTP cables and UTP patch cords should be from same OEM.
3. All the OFC cables and fiber patch cords should be from same OEM.
4. The complete campus network infrastructure implemented under this tender is under comprehensive warranty for 3 years.
5. The bidder should provide the support for the offered products for a period of 10 years from the date of final acceptance. The bidder should submit an undertaking in this regard along with technical bid.
6. The software security patch updates for the offered network switches, firewall should be available until the year 2036 or later. The OEM/Bidder should provide these at no additional cost.
7. Network switches (core, distribution and access) and firewalls should not be declared as end of sale/end of support during the warranty period, bidder should provide the traceability for verification. If any of the product model is declared as end of support/end of sale by the OEM during the warranty period then the bidder should replace the product with the latest model for that item from the same OEM. The Bidder has to provide a duly signed undertaking for the same on non-judicial stamp paper.
8. The installation and configurations of all the active network components (switches, firewalls, SDN appliance and NAC should be performed by CCIE/CCNP certified engineers.
9. Bidder should provide the technical datasheets of all the products and required certification proofs along with the bid.
10. Supplied hardware and software warranty should have back-to-back OEM support, Bidder should submit the required documents from the respective OEMs.
11. All network switches, firewalls, Network access control and SDN system must operate with their full set of features. The bidder shall provide all required licenses with perpetual validity at no additional cost.
12. The proposed solution for campus network infrastructure must be able to scale up or out as required, without significant performance degradation or configuration issues.
13. During the warranty period, on-site technical assistance is to be provided by the bidder/OEM or authorized technical experts within 24 hours, if there is any hardware issue. Bidder has to submit undertaking for the same.

14. The Bidder should agree to repair or replace any parts failed during warranty period with a new one at free of cost. The bidder should note that In Case of storage media (SSD/Flash memory of switches) failure, DMRL will not return the defective storage media for security reasons.
15. During the installation and commissioning process, there should not be any disruptions in existing network connectivity to the end users.
16. Upon successful completion of the installation, the Bidder shall provide the complete copies of all configuration files, as well as the operating system images of all deployed switches and firewalls in a USB storage media/DVD.
17. Upon successful completion of installation, the Bidder shall deploy qualified service engineers for on-site assistance and operations and management for 3 years from the effective date of final acceptance. The deployment shall include L3 Service Engineer, L2 Service Engineer and L1 Service Engineer. Each engineer must possess prior experience and qualifications corresponding to their designated level.
18. Service engineers shall be present at the DMRL premises during office hours, from 08:40 Hrs to 17:10 Hrs, and shall perform duties as directed by the DMRL's IT team. If required the service engineers should be available at DMRL on holidays.
19. In the event of non-compliance, poor performance, or unsatisfactory service by any deployed engineer, the Bidder shall promptly replace the engineer with a suitably qualified expert within 3 days.
20. DMRL reserves the right to encash the Performance Bank Guarantee (PBG) in case of failure by the Bidder to provide satisfactory support during the warranty period.
21. **Payment terms:** Payment for the delivered products (item No 1 to 40), Trenching, HDPE laying & FO cabling with backfilling, Road cutting, trenching and re-cementing and Installation, Configuration, Testing, Commissioning, Training and Documentation will be made after final acceptance.
22. Payment for onsite support for operations, troubleshooting and management of network infrastructure will be made on quarterly basis through PCDA R&D in offline mode after successful completion of job for the quarter.

NON DISCLOSURE AGREEMENT

This agreement made this _____ Day of _____ Month _____ Year between the President of India through the Director, Defence Metallurgical Research Laboratory, (DMRL), Hyderabad hereinafter referred to as "**First Party**" on the one part and the _____ Firm Name with address _____ ("**Second Party**") herein after referred as "**Receiving Party**" which expression shall unless it be repugnant to or inconsistent with subject or context thereof, include and be deemed to include their Heirs, Executors, Successors or Administrators and permitted assigns on the other part.

Hereafter collectively referred to as the "Parties" or individually as the "Party".

WHEREAS, DMRL Hyderabad. (First Party/ Disclosing Party) possess certain sensitive and confidential information and desires to disclose it to the Firm (the Receiving Party) to further co-development relationship between the Parties subject to the Terms and Conditions of this Agreement.

NOW IT IS AGREED AND DECLARED BY AND BETWEEN THE PARTIES AS FOLLOWS:

1. Identification

When Confidential information is disclosed in writing or other tangible form, the information shall be marked "CONFIDENTIAL" or with similar legend on each page containing Confidential information. When Confidential information is disclosed orally, visually or in any other intangible form, such information shall be identified as confidential at the time of disclosure, subsequently summarized and confirmed in writing within Thirty (30) days from the initial disclosure, referring the date of disclosure.

2. Standard of Care

The Receiving Party shall protect the confidential information disclosed by the First Party with appropriate care.

- a. Receiving Party shall communicate to First Party in writing the list of nominated persons for receiving confidential information.
- b. Confidential information should not be communicated through phone, fax, or email. Confidential information should be exchanged only through signed letters.
- c. When confidential information is received by Receiving Party, the Receiving Party should acknowledge the receipt of confidential information in writing.
- d. Receiving Party should not discuss the confidential information disclosed by First Party with any Third Party, within Government Organizations or outside Government Organizations without the prior written approval of Director, DMRL, Hyderabad (First Party). The Firm agrees to promptly notify First Party of any misuse/misappropriation/loss/comprise of the confidential information.

3. Either Party's failure to enforce any provision, right or remedy under this agreement shall not constitute a waiver of such provision, right or remedy.

4. This Agreement will be construed in, interpreted and applied to accordance with the laws of India.

5. Confidentiality Period

For the term of this Agreement and Ten (10) years thereafter, the Receiving Party shall neither disclose the First Party's confidential information to any Party other than its Employees who have express need to know in the context of the relevant co-development.

6. Exceptions

No obligation shall be imposed regarding confidential information if the Receiving Party can demonstrate that the confidential information:

- (a) is or becomes thereafter available to the public through no breach of this Agreement;
- (b) is disclosed pursuant to governmental or judicial order requirement.

7. Return of Materials

The Receiving Party shall return to the First Party, or at the discretion of the First Party certify the destruction of all copies of the First Party's confidential information upon written request of First Party.

8. No License

Nothing herein constitutes a license or other transfer of rights in respect of either Party's interest in any Confidential information disclosed pursuant to this Agreement.

9. Term

The Term of this agreement is Five (5) years from the effective Date, however, those Sections 5, 6, 8 and 11 hereof shall survive even after expiration or termination hereof.

10. Assignment, Modification and Waiver

No assignment, modification, or waiver of any Term of this Agreement shall be effective unless set forth in writing and signed by an Authorized Representative of each Party. No failure to enforce any provision of this Agreement shall be construed as waiver.

11. Dispute Resolution

Difference of opinion, if any, arising during the period of this Agreement, concerning the execution of the responsibilities will be settled on the basis of mutual consultation by the signatories or their designated nominees. The parties will make best possible efforts to resolve the dispute and in case of their failure to do so and reconciling the dispute mutually, the same shall be referred for Arbitration.

12. Arbitration

Any question, dispute or difference arising under the Contract (except as to any matter, the decision of which is specifically provided for) shall be referred to the Sole Arbitration of the Scientific Advisor to Raksha Mantri. It will not be valid objection that the Arbitrator is Government Servant and that he had to deal with the matters to which the Agreement relates or that in the course of his duties as a Government Servant he had expressed views on all or any of the matters, disputes or difference. The Award of the Arbitrator shall be final and binding on both the Parties. The Arbitrator shall be entitled to extend time of award by the consent of the Parties from time to time. The venue of Arbitration shall be New Delhi or any other Place as may be decided by the Arbitrator and the expenses of the Arbitration shall be at the discretion of the Arbitrator. Subject as aforesaid, the Arbitration and Conciliation Act 1996 and the Rules there under and any statutory modification thereof for the time being in force shall be deemed to apply to the Arbitration proceedings under this condition.

13. Entire Agreement

This Agreement constitutes the entire Agreement between the Parties with respect to the matters covered by this Agreement, supersedes all prior agreements and understandings with respect thereof, and may only be amended in writing signed by both Parties.

14. Binding Effect

This Agreement shall be binding and inure to the benefit of the undersigned Parties, their Successors and Assigns.

IN WITNESS WHEREOF, the parties have executed this Agreement to be executed as the effective date written above when signed below by their duly authorized representatives.

For Lab/Estt./First Party

Name :

Designation : Director

Address : DMRL, Hyderabad

Date :

For Firm/Second Party

Name :

Designation :

Address :

Date :

1. Definitions :

In this Non Disclosure Agreement the following terms shall, unless the context otherwise requires, have the following meanings :

1.1 'Disclosing Party' or 'First Party' means DRDO Lab/Estt. disclosing Confidential Information to the Vendor/Seller/Development Partner under this Agreement.

1.2 'Receiving Party' means the Vendor/Seller/Development Partner receiving Confidential Information from DRDO Lab/Estt. under this Agreement.

1.3 'Confidential Information' means any information, which shall include but is not limited to, design, fabrication and assembly drawings, know-how, processes, product specifications, raw materials, product samples, inventions, concepts and any other technical and/or commercial information, disclosed directly or indirectly and in any form whatsoever (including, but not limited to, disclosure made in writing, oral or in the form of samples, models, computer programmes, drawings or other instruments) furnished by the Disclosing Party to the Receiving Party under this Agreement.

1.3.1 Such Confidential Information shall also include but shall not be limited to:

1.3.1.1 information disclosed by the Disclosing Party/First Party in writing marked as confidential at the time of disclosure;

1.3.1.2 information disclosed by the Disclosing Party/First Party orally which is slated to be confidential at the time of disclosure;

1.3.1.3 information disclosed in any other manner is designated in writing as Confidential Information at the time of disclosure; or

1.3.1.4 notwithstanding sub-clauses 1.3.1.1, 1.3.1.2 and 1.3.1.3 of this definition, any information whose nature makes it obvious that it is confidential.

1.3.2 Such Confidential Information shall not include any information which:

1.3.2.1 is, at the time of disclosure, publicly known; or

1.3.2.2 becomes at a later date, publicly available otherwise than a wrongful act or negligence or breach of this Agreement of or by the Receiving Party; or

1.3.2.3 the Receiving Party can demonstrate by its written records was in its possession, or known to the Receiving Party, before receipt under this Agreement, and which was not previously acquired under an obligation of confidentiality; or

1.3.2.4 is legitimately obtained at any time by the Receiving Party from a third Party without restrictions in respect of disclosure or use; or

1.3.2.5 the Receiving Party can demonstrate to the satisfaction of the Disclosing Party, has been developed independently of its obligations under this Agreement and without access to the Confidential Information.

2. Administrative Instructions:

- 2.1** Authority of the Signatory of Receiving Party in NDA shall be established prior to signing of NDA. Preferably, a letter should be obtained from CEO/MD of the Receiving Party authorizing a named senior level official to sign NDA on their behalf. Only such authorised Senior Level Officer should sign the NDA document on behalf of Receiving Party/Second Party.
 - 2.2** The confidentiality of the documents shall also be maintained by the Consortium Partners of the Suppliers/Receiving Party.
 - 2.3** The Labs/Estts./Programmes are advised to enter into this NDA in all Contracts wherein any Confidential Information is being shared with the Receiving Party/Second Party.
-

SCOPE OF PRE-BID MEETING

The pre-bid meeting and associated site visit are intended to provide prospective bidders with a clear understanding of the DMRL's requirements and the site-specific conditions for the supply, installation, and integration of active and passive network components to establish the campus network at DMRL and ATC. The scope includes the following:

Coverage during Pre-Bid Meeting:

1. Provision of existing network architecture diagrams, including fiber layout and endpoint details.
2. Facilitation of a physical site visit for bidders to assess site-specific conditions.
3. In case the site visit cannot be completed on the day of the pre-bid meeting, additional time will be provided to allow all attendees to complete the visit.
4. Discussion of requirements for network monitoring and management dashboards, including functionality and reporting expectations.
5. Discussion of user requirements from network access control system.
6. Upon completion of the pre-bid meeting, a certificate of attendance will be issued to participants, which must be submitted along with the technical bid without exception.

Expectations from Bidders

1. Submit a duly signed Confidential Non-Disclosure Agreement (CNDA) in the prescribed format prior to participating in pre-bid meeting. Submission of the CNDA is a mandatory for participating in the pre-bid meeting.
2. Conduct a site visit prior to bid submission to assess site-specific requirements.
3. Review site layout and existing fiber plans to identify additional accessories or components required for seamless installation and integration.
4. Treat all shared or observed information during pre-bid meeting and site visit as strictly confidential, including physical layout details, existing network infrastructure, and fiber routes.
5. Use the information solely for bid preparation. Bidders shall not disclose, share, reproduce, or disseminate any information obtained during the site visit and pre

bid meeting discussions to any third party, organisation, or individual without prior written consent from DMRL.

6. Any breach of the confidentiality obligations by the bidder or its representatives shall render the bidder liable for immediate disqualification from the tender process, along with any legal action or penalties deemed appropriate by DMRL.

APPENDIX-A**FORMAT FOR DETERMINING LOCAL / NON LOCAL STATUS OF VENDORS
BASED ON TECHNOLOGY CONTENT**

The following table with details of item quoted (without price details) to determine Local / Non-Local content of vendor as per Govt. of India, Ministry of commerce & Industry Notification No. P-45021/2/2017-B.E, dated: 15/06/2017, letter No. P-45021/2/2017-PP(BE-II), dated 04th June 2020 & letter No. P-45021/2/2017-PP(BE-II), dated 16th September 2020(Subject to amendment) & for updated details please refer to www.dipp.gov.in). Bids will be rejected if the price is revealed / displayed in the format.

Sl. No.	Description of Item	% of Indian / Local Technology Content	Location at which Local value addition is made	% of Imported Technology content & Country of origin
01				
	No. of items in the table depends as per the No. of items in scope of supplies attached to Tenders along with specification			

(AUTHORIZED SIGNATURE)

