RailTel Corporation of India Ltd

(A Mini Ratna PSU under Ministry of Railways)

NOTICE INVITING REQUEST FOR PROPOSAL (RFP)

E-EOI/RFP No. : RCIL/EOI/RFP/CO/ITP/2022-23/ IT services to RCIL Customer/10
Dated 20.12.2022

RFP for Selection of Partner for work of

"Implementation of State-of-the-Art ICT Infrastructure on turnkey basis at University Campus in New Delhi"

Issued by:
RailTel Corporation of India Ltd
(A Mini-Ratna PSU under Ministry of Railways)
Corporate Office,
Plate-A, 6th Floor, Office Block Tower-2,
East Kidwai Nagar, New Delhi - 110023,
Ph No. +91-011- 22900600 Fax No. +91-011-22900699
https://www.railtelindia.com

Note: RailTel empanelled partners are only eligible to participate.

Disclaimer

RailTel Corporation of India Ltd. (herein after called the RailTel) has prepared this RFP/EOI/RFP document solely to assist prospective bidders in making their decision of whether or not to bid.

While the RailTel has taken due care in the preparation of information contained herein and believes it to be accurate, neither the RailTel or any of its Authorities or Agencies nor any of their respective officers, employees, agents or advisors give any warranty or make any representations, express or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it. This information is not intended to be exhaustive and interested parties are required to make their own inquiries and do site visits that it may require in order to submit the RFP. The information is provided on the basis that it is non–binding on RailTel, any of its authorities or agencies or any of their respective officers, employees, agents or advisors. The RailTel reserves the right not to proceed with the bidding/EOI/RFP process at any stage without assigning any reasons thereof, or to alter the timetable reflected in this document or to change the process or procedure to be applied. It also reserves the right to decline to discuss the EOI/RFP further with any party submitting an RFP. No reimbursement of cost of any type will be paid to persons or entities submitting the RFP.

TABLE OF CONTENTS

EOI/RFP Notice

RailTel Corporation of India Ltd. (RailTel) invites E-EOI/RFP in Two Packet (Part I –Credential/ Techno commercial Bid and Part II - Price Bid) System for **"**Implementation of State-of-the-Art ICT Infrastructure on turnkey basis in Education University Campus in New Delhi**"**

1	EOI/RFP Document Availability	EOI/RFP document can be downloaded from website https://www.railtel.enivida.com from 20-Dec-2022 onwards till last date of submission of the EOI/RFP.
2	Cost of the EOI/RFP Document	Rs 2,950/- (Including Tax) to be made in favour of RailTel Corporation of India Ltd. online through e-nivida Portal.
3	Earnest Money Deposit (EMD) to be submitted along with EOI/RFP Response	Rs 6,00,000/- to be made in favor of RailTel Corporation of India Ltd. online through e-nivida Portal.
4	Last date of submission of response to EOI/RFP Response	15:00 Hrs on 29-Dec-2022
5	Date & Time of Opening of EOI/RFP Response	15:30 Hrs on 29-Dec-2022

Small scale Units registered with NSIC/MSME under single point registration scheme are exempted from cost of Tender Documents and EMD. No other relaxations will be given.

Note: EOI/RFP Notice and EOI/RFP Document are available on RailTel's website and can be downloaded from **www.railtelindia.com** or from the e-Tendering portal https://railtel.enivida.com/. For online bid submission the bidder will have to necessarily download an official online copy of the EOI/RFP documents from e-nivida portal. All future Information viz. corrigendum /addendum/ amendments etc. for this Tender shall be posted on the e-Tendering Portal only. Printed copy of Tender document will not be sold from RailTel office.
The bidder shall bear all costs associated with the preparation, submission/participation in the bid. Purchaser in no way will be responsible or liable for these costs regardless of the conduct or outcome of the bidding process.

Contact Details for this EOI/RFP :

Rajeev Kumar / Dy. General Manager (ITP) / rajeevkumar@railtelindia.com

Ph No. +91-011- 22900600 **Fax No.** +91-011-22900699

General Manager/ITP

1. About RailTel

RailTel Corporation of India Ltd (RailTel) is one of the largest neutral telecom infrastructure providers in the country owning a Pan-India optic fibre network on exclusive Right of Way (ROW) along Railway track. The OFC network presently reaches to over 4500 towns & cities of the country including several rural areas. With its Pan India high-capacity network, RailTel is working towards creating a knowledge society at various fronts. The portfolio of services provided by RailTel includes Data Centre & DR services, Tele-presence as a service, NLD services, IP-1 services, Internet and Broadband services on a pan-India basis.

Equipped with an ISO 9001, 20000-1:2011 & 27000 certification, RailTel offers a wide gamut of managed telecom services to Indian Telecom market including Managed lease lines, Tower colocation, MPLS based IP-VPN, Internet, Data Centre services, NGN based voice carriage services to Telecom Operators, Dark fibre leasing to MSOs/LCOs. The major customer segment for RailTel comprises of Enterprises, Banks, Government Institutions/Department, Educational Institutions/Universities, Telecom Service Providers, Internet Service Providers, MSOs, etc. RailTel being a "Mini Ratna (Category-I)" PSU is steaming ahead in the enterprise segment with the launch of various services coupled with capacity augmentation in its Core network.

2. Scope of Work

RailTel is providing Project management consultancy services to one of its government customer (education university) for Designing, Planning, Monitoring and Supervising the Implementation of State-of-the-Art ICT Infrastructure on turnkey basis at their newly built campus in New Delhi; followed by Monitoring and Supervision of Operations, Management and Maintenance of the implemented ICT infrastructure. RailTel requires a suitable empanelled partner for execution of works as detailed in Annexure-1 " Scope of work".

3. Partner Selection methodology

3.1. Interested partners shall understand the overall Scope of Work.

3.2. Interested partners need to submit their online EOI/RFP response on E-Nivida Tendering portal of RailTel. Directions regarding E-Nivida portal are provided in EOI/RFP document under "E-tendering Instructions to Bidders"

3.3. The technical bid will be examined for the required documents as mentioned in this EOI/RFP. The bid should be digitally signed by the authorised signatory of the organization. RailTel may further ask for submission of supplement / additional documents for arriving on whether the bid can be termed as 'technically qualified or not'. The interested partners must submit the supplement / additional documents, as and when asked by RailTel and within the time frame as mentioned by RailTel, else their bid will be termed as 'non-responsive' and will be termed as 'technically disqualified' without issuing any further notice

3.4. The interested partners, who have submitted their Tender response within the stipulated time, and whose technical bid is found to be in place as per the requisites mentioned in this EOI/RFP document, will be termed as 'Technically Suitable Partners (hereafter referred to as 'TSP') and they will be communicated accordingly. Commercial bid of only such TSP(s) will be further opened. The bid evaluation shall be done on Quality–cum–Cost Based Selection (QCBS) as per details provided under clause number 4.

3.5. The TSP, The bid of the bidder, who obtains the highest T value, will be rated as the Most Responsive Bid and will be declared as 'Commercially Suitable Partner (hereafter referred to as 'CSP')'. Further, RailTel reserves the right to have negotiation with the CSP.

3.6. Validity of the submitted bid (technical and commercial) should be of 120 days from the last date of submission of EOI/RFP response as mentioned in this EOI/RFP document.

4. EOI/RFP Evaluation Criteria:

Process of Evaluation: The bid evaluation shall be done on Quality–cum–Cost Based Selection (QCBS).

The technical bid marks (TS) shall be assigned to each bid on the basis of following evaluation matrix.

The Technical Bid Score "TS" of the Bidder shall be derived as under:

TS = (TM / TH) x 100

Where:

TS is the Technical Bid Score

TM= Total Technical bid marks of the bidder under consideration

TH= Highest total Technical bid marks amongst all evaluated bids

Technical Evaluation:

Criteria	Max Criteria/ Sub Criteria Marks
Company Profile	**20**
Relevant experience	**30**
Solution Proposed, Approach & Methodology	**30**
Technical Presentation	**20**
Total Points	**100**
Minimum Marks	**60**

At any time during the process of evaluation the Bid Evaluation Committee may seek specific clarifications from any or all Bidders.

Evaluation of Financial Bids:
In this phase, the Financial Bids of the Bidder, who are technically compliant and who have scored more than 60% marks in Technical Evaluation shall be opened. Formula to determine the scores for the Financial Bids shall be as follows.

FS= (FL/F) x 100
Where:
FS is the Financial Score of Price submitted under consideration.
FL is the total value of the lowest Commercial Bid under consideration.
F is the total price quoted in the bid under consideration.

Combined Evaluation of Technical & Financial Bid:

Technical Score shall be given 70% weight-age in total score and Financial Score shall be given 30% weight-age in total score as described below:

- The Total score of the Bidder will be determined as under:

Total Score = (T) = (0.7 x TS) + (0.3 x FS)

- The bid of the bidder, who obtains the highest T value, will be rated as the Most Responsive Bid. In the event of the same T score of bidders, the bid with the highest Technical score (TS) will be rated as the most responsive bid.

Note: The evaluation shall be separate for SOR A and SOR B, hence separate PO can be issued to two different bidders.

Detailed technical evaluation criteria score as per table given below:

S. No.	Criteria/Sub Criteria	Point System	Max marks
A	**Company Profile**		**20**
A.1	Annual average turnover of bidder in INR during the last 3 financial years, i.e. 2019-2020, 2020-2021 & 2021-2022 from IT/ ICT infrastructure projects. Copy of Annual report & Statuary Auditor certificate.	**When revenue turnover is:** equal to or more than INR 1000 Cr : 10 marks 701-1000 Cr : 8 Marks 501-700 Cr : 6 Marks 401-500 Cr.: 4 Marks 107-400 Cr : 2 Marks	10
A.2	Bidder having Certifications: i. ISO 20000-1: 2013 or latest ii. ISO 27001: 2013 or latest iii. CMMi3 or above	Bidders having all three the certificates – 8 Bidders having CMMI L5 certificate – additional 2 Marks	10
B	**Relevant Experience**		**30**
B.1	The bidder must have successfully completed at-least one project of supply, installation and commissioning of Data Centre, Networking IT infrastructure products having minimum project value of INR 25 crores of each project for Central / State Governments/ PSUs/Corporate in last 5 years as on date of bid submission.	Two or More than 2 projects: 10 marks 1 project: 6 marks	10
B.2	Implementation of Projects like Data Centres / NOC / SOC. The value of implementation of the single project should be minimum Project 25 Crores for technical works including Equipment & physical infrastructure works (excluding civil works) etc. for Central / State Governments/ PSUs/Corporate as on date of bid submission.	Value of the single project equal to or more than 250 Cr.: 10 marks Value of the single project more than 100 Cr to less than 250Cr.: 8 marks Value of the single project is 25-100 Cr.: 5 marks	10
B.3	Bidder should have at least completed 1 year of Operations and Maintenance of ICT infrastructure like Data Centre / NOC /SOC / Networking etc in last 5 years as on	2 or More than 2 projects: 10 marks 1 Project: 6 marks	10

	date of bid submission. with any Central / State Governments/ PSUs/Corporate.		
C	**Solution Proposed, Approach & Methodology**		**30**
C.1	Proposed Solution	Technical Solution	10
C.2	Approach and Methodology	Approach Note	10
C.3	Product suitability and proven ness	Technical Solution	10
D	**Technical Presentation**		**20**
	Total Points		**100**

5. Qualification for Interested Partner

S. No.	Pre-qualification Criteria	Mandatory documentary evidence to be submitted
1	The interested partner should be an Empanelled Partner with RailTel on the date of bid submission.	a) Copy of "Letter of Intent" of empanelment
2	The interested partner should submit duly signed and stamped EOI/RFP cover letter as per the format mentioned at Annexure-01 of this EOI/RFP document.	a) duly signed and stamped EOI/RFP cover letter
3	The interested partner should submit Earnest Money Deposit (EMD). Tender response without 'EMD is liable for rejection without assigning any further notice.	a) EMD of Rs. 6 Lakhs
4	The interested partner should be in compliance to insertion of Rule 144(xi) in the GFR, 2017 vide office OM no. 6/18/2019-PPD dated 23-July-2020 issued by Ministry of Finance, Government of India, including revisions.	a) Self-declaration is to be submitted in this regard.
5	The interested partner should submit an undertaking for maintaining of 'Local Content Compliance' (refer Clause No. 3.7. above).	a) submit a certificate mentioning the 'Local Content Percentage' duly signed and stamped by statutory auditor or cost auditor of interested partner.
6	There should not be any ongoing or past, arbitration case(s) between 'RailTel or CUSTOMER or Organizations under Indian Railways' and 'Interested Partner' on the last date of submission of EOI/RFP.	a) Self-Declaration is to be submitted in this regard
7	Integrity Pact (02 Set) in original duly signed and executed on stamp paper of appropriate value in the format as mentioned in this Tender document.	a) Duly signed Integrity Pact (02 Set)
8	The interested partner should have a valid Goods and Service Tax Identification Number (GSTIN), as on the last date of submission of EOI/RFP.	a) Copy of documents in this regard is to be submitted.
9	The interested partner must be an established Company registered under the – Indian Companies Act, 1956/2013, or partnership firm register under LLP Act, 2008 since last 5 years as on 31st March 2022.	a) Copy of Certificate of Incorporation b) Copy of Registration Certificate

S. No.	Pre-qualification Criteria	Mandatory documentary evidence to be submitted
10	Bidder should have minimum annual average turnover of INR 107 Crores from similar work including Data Centre, networking, Telecom activity during the last 3 financial years ending 31st March 2022.	Audited accounts of the company as filed before the Registrar of Companies. Or Certificate to this effect from the CA of the company.
11	The Net Worth of the bidder must be positive for each of the last 3 financial years ending 31st March 2022.	Certificate to this effect from the CA of the company.
12	The bidder must have successfully completed at least 1 project of supply, installation and commissioning of Data Centre, Networking IT infrastructure products having minimum Project value of INR 25 crores for Central / State Governments/ PSUs/Corporate in last 5 years as on date of bid submission.	Copy of work order(s) / Purchase Order/ Completion Certificate/ contract agreement. Supported with relevant documentary evidences Completion or Go Live or FAT certificates by the customer to be submitted as evidence
13	Implementation of Projects like Data Centers / NOC / SOC. The value of implementation of the single project should be minimum INR 25 Crores for technical works including Equipment & physical infrastructure works (excluding civil works) etc. for Central / State Governments/ PSUs/Corporate as on date of bid submission.	Copy of work order(s) / Purchase Order/ Completion Certificate/ contract agreement. Supported with relevant documentary evidences Completion or Go Live or FAT certificates by the customer to be submitted as evidence
14	Bidder should have completed at-least 1 year of Operations and Maintenance of ICT infrastructure like Data Centre / NOC /SOC / Networking etc in last 5 years as on date of bid submission. with any Central / State Governments/ PSUs/Corporate.	Copy of work order(s) / Purchase Order/ Completion Certificate/ contract agreement. Supported with relevant documentary evidences Completion or Go Live or FAT certificates by the customer to be submitted as evidence. In case of comprehensive PO including SITC as well as O&M, in such case the O&M portion in PO must be clearly identified on PO and completion certificate.
15	The bidder must possess, at the time of bidding, a valid ISO 27001, ISO 20000 and CMMI Level 3	Copy of certification which is valid on date of bid Submission.
16	Any organization debarred / black-listed by Central / State Government in India, for last 3 years at the time of submission of the RFP, shall not be allowed to participate in this EOI/RFP. Bidder need to submit a self certification in this regard.	A Self Certified letter as per < format ...>: Self-Declaration
17	The bidder should have on its roll at least 200 ICT Professionals as its direct employees as on the date of bid submission (Staff performing duties of Data Centre and Network Design, Implementation, Installation, Testing and maintenance activities)	Certificate from the authorized signatory of the company
18	Bidder should: - a) not be insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons; b) not have, and their directors and officers not	A Self Certified letter as per < format ...>: Self-Declaration

S. No.	Pre-qualification Criteria	Mandatory documentary evidence to be submitted
	have, been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of five years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings; c) not have a conflict of interest in the procurement in question as specified in the bidding document. d) comply with the code of integrity as specified in the bidding document.	
19	All items proposed under solution by bidder shall have 5 years OEM warranty from date of issue of PAC.	Undertaking for 5 years warranty on company letterhead
20	The interested partner should have active partnership with OEM of all major items.	Proof of active partnership with OEM. For small items self undertaking of partnership with OEM can be submitted.

Note: EOI/RFP response submitted in form of Consortium / Partnership shall be rejected.

6. Proposal Preparation and Submission Cost

The interested partner is responsible for all costs incurred in connection with participation in this EOI/RFP process, including, but not limited to, cost incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal, in providing any additional information required by RailTel to facilitate the evaluation process or all such activities related to the bid process. RailTel will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process. This EOI/RFP document does not commit to award a contract or to engage in negotiations.

7. Amendment to EOI/RFP Document

At any time prior to the deadline for submission of bids, RailTel, may, for any reason can modify the EOI/RFP document by an amendment. All the amendments made in the document would be informed by displaying on RailTel's (www.railtelindia.com) and E-Nivida website only. The interested partners are advised to visit the RailTel website on regular basis for checking necessary updates. RailTel also reserves the rights to amend the dates mentioned in this EOI/RFP for bid process. RailTel may, at its discretion, extend the last date for receipt of Tender response

8. Bid Validity Period

8.1. Bid of Interested partners shall remain valid for the period of 120 days from the date of submission of EOI/RFP, as mentioned in this EOI/RFP document.

8.2. RailTel may request the for an extension of the period of validity. The request and the responses thereto shall be made in writing through e-mail communication only. Further, whenever the bid validity extension is submitted by the interested partner, it should be ensured by interested partner that their PBG related to the empanelment should have minimum validity of 90 days from the last date of extended bid validity period.

9. Right to Terminate the Process

RailTel may terminate the EOI/RFP process at any time without assigning any reason. RailTel makes no commitments, express or implied, that this process will result in a business transaction with anyone. This EOI/RFP does not constitute an offer by RailTel. The interested partner's participation in this process may result in RailTel selecting the CSP to engage in further discussions and negotiations toward execution of a contract. The commencement of such negotiations does not, however, signify a commitment by RailTel to execute a contract or to continue negotiations. RailTel may terminate negotiations at any time without assigning any reason.

10. Language of Bid

The bid prepared by the interested partner and all correspondence and documents relating to the bids exchanged by the bidder and RailTel, shall be written in English Language, provided that any printed literature furnished by the Bidder in another language shall be accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall govern. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the Authorised Signatory of the interested partner. Submission of Bid

11. Submission of Bid

11.1. The interested partner should take into account any Corrigendum to this EOI/RFP document that may have been published before submitting their EOI/RFP response. The bid is to be submitted in the mode as mentioned in this EOI/RFP document. EOI/RFP response submitted in any other mode will not be entertained.

11.2. Interested partners in their own interest are advised to submit the EOI/RFP response well in time before the last date and hence to avoid any inconvenience at the last moment.

11.3. An Organization / Interested Partner can submit only 'One EOI/RFP Response'. Submission of multiple EOI/RFP Response by interested partner(s) may lead to rejection of all of its bid.

12. Rights to Accept / Reject any or all EOI/RFP Response

RailTel reserves the right to accept or reject any EOI/RFP Response, and to annul the bidding process and reject all Bids at any time prior to award of the Contract, without thereby incurring any liability to the affected interested partner(s) / TSP(s) / CSP, or any obligation to inform the affected Bidders of the ground for RailTel's action.

13. Warranty

13.1. The warranty would be valid for a period of 5 years from last PAC issued to selected bidder in contract. The supplier shall warrant that stores to be supplied shall be new and free from all defects and faults in material, workmanship and manufacture and shall be of the highest grade and consistent with the established and generally accepted standards of materials of the type ordered and shall perform in full conformity with the specifications and drawings. The supplier shall be responsible for any defects that may develop under the conditions provided by the contract and under proper use, arising from faulty materials, design or workmanship such as corrosion, inadequate quantity of material to meet equipment requirements, inadequate contact protection, deficiencies in design and/ or otherwise and shall remedy such defects at his own cost when called upon to do so by the Purchaser who shall state in writing in what respect the stores are faulty.

13.2. If it becomes necessary for the contractor to replace or renew any defective portion/portions of the supplies under this clause, the provisions of the clause shall apply to the portion/portions of the equipment so replaced or renewed or until the end of the above-mentioned period or twelve months, whichever may be later. If any defect is not remedied within a reasonable time of 30 days, the Purchaser may proceed to do the work at the contractor's cost, but without prejudice to any other rights which the Purchaser may have against the contractor in respect of such defects.

13.3. Replacement under warranty clause shall be made by the contractor free of all charges at site including freight, insurance and other incidental charges.

Note- Warranty and Support of all product/solution supplied must be available for 5 years from the date of last PAC issued to selected bidder. Selected bidder shall submit OEM undertaking on warranty certification along with the statement that Products/Solutions supplied against this tender shall not be end of life/end of support for next 5 years from the date of PAC. In any exceptional circumstances, if supplied product are being phased out by OEM, product with similar or higher version/specifications will be supplied by bidder without any Cost to RailTel.

The Warranty shall be Onsite Warranty and shall be Comprehensive and shall include free maintenance of all the supplied equipment, devices, infrastructure, softwares, etc. with free replacement of equipment, infrastructure, devices, parts, softwares thereof including free software upgrades/updates/renewals, etc."

The Successful bidder shall provide back-to-back written warranty from the OEM of the supplied Equipment, devices, Infrastructure, softwares, etc. so as the OEM shall ensure compliance of this warranty clause in case the bidder defaults at any point of time during the period of Warranty.

13.4. Warranty Support

13.4.1. Material for repair during Warranty Period shall be handed over /taken over to contractors engineer at Customer location.

13.4.2. During the warranty period, the contractor shall be responsible to the extent expressed in this clause for any defects that may develop under the conditions provided for by the contract and under proper use, arising from faulty materials, design or workmanship in the plant, or from faulty execution of the plant by the contractor but not otherwise and shall remedy such defects at his own cost when called upon to do so by the Purchaser Engineer who shall state in writing in what respect the portion is faulty.

13.4.3. During the free warranty maintenance period contractor should stabilize the working of the system. Purchaser has the right to extend the period of supervision of the maintenance free of cost till the system stabilizes and works satisfactorily for a reasonable period of time. If during the time any equipment etc. is to be added or deficiencies are to be rectified to make the system work trouble free the same also will have to be done by the contractor at no cost to RailTel as to make good, all the deficiencies.

14. Delivery Period

The complete infra solutions as per SOR are required to be delivered within period of 6 months from date of award of contract. The bidder shall provide 5 years warranty.

15. Variation in Contract

+/-25% variation may be operated on SOR value during the period of Project Schedule with the approval of competent authority with similar terms and procedure as specified in the agreement.

16. Payment Terms:

Selected bidder shall raise tax invoices and submit to RailTel as per payment milestones, on basis of which RailTel will generate and submit its invoice for submission to Customer. RailTel shall be receiving payment from customer within 30 days. RailTel will release the payment to selected bidder only after receiving of payment from customer on '**back-to-back**' basis within 7 days and in case of any deduction same shall be passed on to the selected bidder. For MSME payment the due date shall be started from the date of actual payment by customer to RailTel.

16.1. 80% payment of the value of the supply items would be made on receipt of material by the consignee (at customer location) duly inspected and on submission of the following documents subject to any deductions or recovery which RailTel may be entitled to make under the contract:

- Original Tax Invoice. (With separate Tax amount, containing POS, RailTel GSTN and Vendor GSTN).
- Delivery Challan.
- Original Consignee receipt.
- Warranty Certificate of OEM.
- Copy of Submitted Performance Bank Guarantee (PBG)
- GSTN of Ship to location will be used

16.2. 15% payment of the value of Supply items of the PO/LOA shall be made on successfully completion of Installation, Configuration, Implementation & testing of the supplied solution and after stabilization of supplied solution at least 1 month period and on issuance of Provisional Acceptance Certificate (PAC) which will be issued after the completion of entire scope within each building. Separate PAC shall be issued for each building work completion.

16.3. The last 5% payment of the value of Supply items of the PO/LOA shall be made by RailTel on issue of Final Acceptance Certificate (FAC).

16.4. For Manpower O&M (Opex): The O&M period of 4 years shall start with effect from date of issue of FAC. Payment of O&M Manpower charges shall be paid to selected firm on quarterly basis during O&M period of 4 years in equal installments.

16.5. Accounting unit/bill passing unit for the supplies under SOR is Corporate Office. Bills to be submitted to the GM/ITP for passing for payment. The bidder will submit certifying receipt of material & services issued from consignee/regions, for passing for payment. The breakup of taxes has to be furnished and same should be reflected in the bills so that any GST credit can be availed by RailTel.

17. Mobilization Advance payment from Customer:

In case RailTel receives some %age of advance payment from Customer in lieu of project mobilization advance, the same %age of advance can be paid to selected bidder at a simple interest of 10% based on RailTel PO value after submission of separate bank guarantee of advance amount to RailTel. The advance payment shall not exceed 20% of total contract value.

18. Performance Bank Guarantee (Security Deposit)

18.1. The successful bidder has to furnish security deposit in the form of Performance Bank guarantee @ 3% of issued PO/ LOA value, the same should be submitted within 30 days of issue of LOA/PO, failing which a penal interest of 15% per annum shall be charged for the delay period i.e. beyond 30 (thirty) days from the date of issue of LOA/PO. This PBG should be from a Scheduled Bank and should cover FAC plus four months for lodging the claim. The performance Bank Guarantee will be discharged by the Purchaser after completion of the supplier's performance obligations under the contract. The validity period of initial PBG shall be 1 year plus 4 months after issuance of FAC. The claim period for submitted PBG should be one year from the date of expiry. The PBG validity period can be taken as 22 months (6 months delivery period + 12 months support period after last PAC issuance + 4 months). In case of delay in delivery or FAC period, the PBG is also required to be extended accordingly.

18.2. The earnest money shall be released on submission of PBG. The Performa for PBG is given in Chapter 6 Form No. 1. If the delivery period gets extended, the PBG should also be extended appropriately.

18.3. The Performance Bank Guarantee (security deposit) will bear no interest.

18.4. This PBG would be released after satisfactory completion of contract including warranty period plus 4 months.

18.5. A separate advice of the BG will invariably be sent by the BG issuing bank to the RailTel's Bank through SFMS and only after this the BG will become acceptable to RailTel. It is therefore in own interest of bidder to obtain RailTel's bank IFSC code, its branch and address and advise these particulars to the BG issuing bank and request them to send advice of BG through SFMS to the RailTel's Bank.

18.6. On completion of initial PBG, selected bidder is required to submit separate maintenance PBG @ 3% of 25% of PO value which shall be valid uptill completion of 4 years O&M period plus 4 months. The separate PBG is required to be submitted before expiry of initial PBG. On submission of separate PBG, selected bidder' s initial PBG can be returned back on basis of supplier's performance obligations.

19. Taxes & Duties:

19.1. The price quoted in the offer should be firm, fixed indicating the break up and inclusive of all taxes and duties like import, custom, anti-dumping, CGST, IGST, SGST, UTGST etc. The offer should be inclusive of packing, forwarding, freight up to destination, insurance charges.

19.2. Bidder shall issue valid tax invoice to RailTel for availing proper credit of CGST/SGST/IGST/UTGST in case of award of contract. GST will not be reimbursed in the absence of valid tax invoice.

19.3. For all the taxable supplies made by the vendor, the vendor shall furnish all the details of such taxable supplies in the relevant returns to be filled under GST act.

19.4. If the vendor fails to comply with any of the above, the vendor shall pay to purchaser any expense, interest, penalty as applicable under the GST act.

19.5. In case of incorrect reporting of the supply made by the vendor in the relevant return, leading to disallowance of input credit to purchaser, the vendor shall be liable to pay applicable interest under the GST act to the credit of purchaser. The same provisions shall be applicable in case of debit/credit notes.

19.6. Tenderer shall quote all-inclusive rates, but there shall be break up of basic price and all type of applicable taxes such as SGST/CGST/IGST/UTGST along with respective HSN/SAC code under GST law (Including tax under reverse charges payable by the recipient).

19.7. Wherever the law makes it statutory for the purchaser do deduct any amount towards GST at sources, the same will be deducted and remitted to the concerned authority.

19.8. The imposition of any new tax and/or increase/ in the aforesaid taxes, duties, levies, after the last stipulated date for the receipt of tender including extensions if any and the bidder there upon necessarily and properly pays such taxes/levies/cess, the bidder shall be reimbursed the amount so paid, provided such payments, if any, is not, in the opinion of RailTel attributable to delay in execution of work within the control of bidder. The bidder shall within a period of 30 days of the imposition of any such tax or levy or cess, give a written notice thereof to RailTel that the same is given pursuant to this condition, together with all necessary information including details of input credit relating thereto. In the event of no payment/default payment of any of the above taxes, RailTel reserves the right to withhold the dues/payments of bidder and make payment to states/central government authorities as may be applicable. However, if the rates are reduced after the last stipulated date for receipt of tender, bidder has to pass on the benefits to RailTel.

19.9. In case of imported equipment:
Anti-Dumping duty if applicable on the equipment proposed to be supplied by OEM/Tenderer as per extant instructions of Ministry of Commerce/Finance Government of India, has to be borne by the tenderer and shall be deducted from the amount payable to the bidder at the time of making payment to the firm, if this duty amount is paid to custom Authority by RailTel.

Inter se position of the offers will be determined on total unit rate on CIP destination basis which will include basic rate, custom duty, CGST, SGST, IGST, UTGST, freight, Insurance and any other charges or cost quoted by the tenderer, including GST payable on reverse charge by RailTel, whenever applicable.

In regards to works contract, the tenderer should have registration no. for GST in respective state where work is to be executed and shall furnish GST registration certificate on award of LOA.

19.10. Tax details of RailTel Customer: The Education University has been extended the Privileges and Immunities under Section '3' of the United Nations (Privileges and Immunities) Act, 1947 by the Government of India. The University is exempted from paying and collecting all Direct and Indirect Taxes in India. In terms of Article4(1) of the Agreement among SAARC Nations for establishment of Education University, "the (Education) University and its campuses and centres shall be exempted, in the state where they are located, from paying and from collecting all direct and indirect forms of taxes and duties for the establishment and operations of the University". In terms of Section-3 of the

Education University Act 2008 (Act No. 8 of 2009) passed by the Parliament of the Republic of India, notwithstanding anything contrary contained in any other law, the provisions of the above referred Agreement among SAARC Nations for establishment of Education University shall have the force of law in India.

Accordingly, to give effect to tax exemption status of the Education University for Implementation of State-of-the-Art ICT Infrastructure in its campus at Maidan Garhi, New Delhi, the bid price may be inclusive of GST but exclusive of Service Tax and Customs, as per details given below.

Being an International organization as per notification under section 3 of UN (Privilege and Immunities) Act, 1947; the University is exempt from paying custom duty and wherever necessary the bidder will be provided with appropriate certificates to that effect. Therefore, as far as possible, the successful bidder will try to procure goods in a manner that will allow the University to avail of the benefit of customs duty exemption. Selected bidder will inform the University when importing goods. Goods will be cleared by the Customs House Agent (CHA) of the University without paying any custom duty; however, CHA charges will be borne by the bidder.

The GST on imports is not to be paid as the exemption certificate from the Protocol Division of the Ministry of External Affairs will be obtained by the University while goods are ordered. The ordering will be done by the bidder on behalf of, and in the name of, the University.

20. Liquidated Damages

The timely delivery is the essence of this tender. Liquidated damages will be applicable at the rate of half percent (including elements of taxes, duties, freight, etc.) per week or part thereof for undelivered portion of SOR subject to a maximum of 10% of the cost of Purchase order for any reason whatsoever attributed to failure of tenderer. RailTel will have the right to cancel the order, place order on alternative source besides levying the liquidated damages as above.

21. Bid Earnest Money (EMD)

21.1. The bidder shall furnish a sum as given in EOI/RFP Notice as Earnest Money through online transaction in favour of "RailTel Corporation of India Limited" payable at Delhi which should remain valid for 120 days beyond the bid opening date.

21.2. The EMD may be forfeited if a bidder withdraws his offer or modifies the terms and conditions of the offer during validity period and in the case of a successful bidder, if the bidder fails to accept the Letter of Acceptance (LOA) and fails to furnish performance bank guarantee (security deposit) in accordance with clause 12.

21.3. Offers not accompanied with valid Earnest Money shall be summarily rejected.

21.4. Earnest Money of the unsuccessful bidder will be discharged / returned as promptly as possible but not later than 30 days after the expiry of the period of offer / bid validity prescribed by the Purchaser.

21.5. The successful bidder's EMD will be discharged after the first payment to selected bidder and after deduction of Security deposit amount as per clause 12.

21.6. Earnest Money will bear no interest.

21.7. For Micro and Small Enterprises (MSEs)

21.7.1. Certain benefits/preferential treatment shall be extended to the registered MSEs as per guidelines issued in the latest notification of Ministry of MSME/ Government of India.

21.7.2. MSEs who are interested in availing themselves of these benefits will enclose with their offer the proof of their being MSE registered with any of the agencies mentioned in the notification of Ministry of MSME.

21.7.3. The MSEs must also indicate the terminal validity date of their registration

21.7.4. Failing 20.7.2 3and 20.7.3 above, such offers will not be liable for consideration of benefits detailed in the notification of Government of India.

21.7.5. The due date of payment shall be considered as the date of receipt of payment from Customer to RailTel.

22. Preference to make in India:

The provisions of the revised "Public Procurement (Preference to Make in India) Order 2017" dated. 15.06.2017 & dated 16.09.2020 (or subsequent revisions, if any till opening of tender) by Department of Promotion of Industry and Internal Trade (DPIIT), GoI shall apply to this tender.

22.1. Local Content:

i. Only Class-I local suppliers (meeting minimum 50% local content) & Class-II local suppliers (meeting minimum 20% local content) are eligible to participate in this tender.

ii. Minimum Local Content shall be 50% for purchase preference or as per the Notification No. 18-10/2017-IP dated 29th August 2018 issued by Department of Telecommunications, Ministry of Communications and Notification No. 33(1)/2017-IPHW dated 14.09.2017issued by MeitY or latest notification issued till opening of tender.

iii. Among all qualified bids, the lowest bid will be termed as L1. If L1 is Class-I local supplier, the contract will be awarded to L1. If L1 is not Class-I local supplier, the lowest bidder among the Class-I local supplier, will be invited to match the L1 price subject to local supplier's quote price falling with in the margin of purchase preference of 20%, and the contract shall be awarded to such Class-I local supplier subject to matching the L1 price. In case such lowest eligible Class-I local supplier fails to match the L1 price, the Class-I local supplier with the next higher bid within the margin of purchase preference of 20%, shall be invited to match the L1 price and so on and contract shall be awarded accordingly. In case none of the Class-I local supplier within the margin of purchase preference of 20%, matches the L1 price, the contract may be awarded to the L1 bidder. Please refer clause-4.A.41.1 of Chapter-4Aof this tender.

iv. As per para 9 of PPP-MIII order 16.09.2020, bidder shall be required to indicate percentage of local content and provide self-certification in his bid (without mention of any price) that the item offered meets the local content requirement for Class-I/Class-II local supplier, as the case may be and shall also give details of the location(s) at which the local value addition is made. In case of procurement for a value in excess of Rs. 10 Crores, the bidder shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. Bidder shall upload the certificate along with their techno-commercial bid. The bidder shall also provide calculation of Local Content with price Break-up of "Local Content" and "Imported Content" for each SOR item as per DPIIT's PMI Policy and its clarifications and same shall be uploaded by the bidder along with their price bid. In case of any false declaration, action shall be taken in line with the provisions of the PPP-MIII order. Performa for self-certification regarding local content is given in the Notification No. 18-10/2017-IP dated 29th August 2018 issued by Department of Telecommunications.

v. Self-certification of bidder as above shall be supported by the following certificate form Statutory Auditor engaged by the bidder, on the letter head of such Statutory Auditor. "We_____ the statutory auditor of M/s.__ (name of the bidder) hereby certify that M/s._____ (name of bidder) meet the mandatory Local Content requirements of the Project Work under this tender i.e. __% (to be filled by the work center) quoted vide offer No._____ dated___ against RAILTEL tender No._____ by M/s. _____ (Name of the bidder).

Note: In case of bidder(s) for whom Statutory Auditor is not required as per law, required certificates shall be provided by a practicing Chartered Accountant.

vi. Office Memorandum Dated 19.02.2020 (or latest) issued by Department of Telecommunications, Ministry of Communications shall be applicable for Clause 10(d) of Public Procurement (Preference to Make in India) Order, 2017.

vii. Official website of Department of Promotion of Industry and Internal Trade (DPIIT) i.e. "https://dpiit.gov.in/public-procurements" may be referred by tenderers for above mentioned orders or any revision issued. Frequently Asked Question (FAQ) available there may also be referred by tenderers.

21.1.1. Bidders sharing a land border with India:

Office Memorandum F.No.6/18/2019-PPD dated 23.07.2020 by Ministry of Finance, Department of Expenditure, Public Procurement Division shall also apply to this tender. A certificate as per Annexure-I shall be submitted by all the bidders regarding their compliance with this order. If such certificate given by a bidder whose bid is accepted is found to be false, this would be a ground for immediate termination and further legal action in accordance with law. Registration should be valid at the time of submission of bids and at the time of acceptance of bids. In respect of supply otherwise than by tender, registration should be valid at the time of placement of order.

23. System Performance Guarantee

23.1. The tenderer shall give unqualified and unconditional guarantee that when the Infra Solution supplied by firm is installed and commissioned at site, it shall achieve the desired objective and that in the event of performance of the system when installed not complying with the end objective or with the specifications, firm shall provide further inputs to enable the RailTel to realize the end objectives with full compliance of the specifications contained in these documents. No additional payment will be made to the contractor for supply of any additional goods and service required in this regard.

23.2. This certificate in the Proforma given in **Form No. 2**, shall accompany the final offer. Absence of this certificate which will form part of the agreement shall disqualify the tenderer automatically.

24. Integrity Pact (IP) Program

24.1. RailTel has adopted Integrity Pact Program and for implementation thereof all EOI/RFPs relating to procurement of OFC, quad cable, pre-fab shelters, electronic equipment and its installation and/or commissioning etc and other item(s) or activity/activities proposed to be carried out or required by the Company for the value ex-ceding Rs. 15 crores at a time including for repair and maintenance of cable/network and any other items required for special works assigned to RailTel will be covered under the Integrity Pact Program and the vendors are required to sign the IP document and submit the same to RailTel before or along with the bids.

24.2. Only those vendors who have purchased the EOI/RFP document and signed the IP document can send their grievances, if any, to the Independent External Monitors (IEMs) and the nodal officer, i.e. Chief Vigilance Officer (CVO), RailTel.

Name of IEMs and contact details:

1. Mrs. Vinit Kumar Jayaswal — E-Mail: gkvinit@gmail.com
2. Sh. Punati Sridhar — E-mail: poonatis@gmail.com

Name & Contact details of Nodal Officer (IP) in RailTel:

Chief Vigilance Officer
RailTel Corporation of India Ltd.
Plate-A, 6th Floor, Office Block Tower-2,

East Kidwai Nagar, New Delhi - 110023
e-mail: cvo[at]railtelindia[dot]com

24.3. If the order, with total value equal to or more than the threshold value, is split to more than one vendor and even if the value of PO placed on any/each vendor(s) is less than the threshold value, IP document having been signed by the vendors at bid stage it- self, the Pact shall continue to be applicable.

24.4. Bidder of Indian origin shall submit the Integrity Pact (in 2 copies) on a non-judicial stamp paper of Rs. 100/- or the appropriate value (as the case may be), duly signed by the person signing the bid. If the bidder is a partnership or a consortium, the Integrity Pact shall be signed by all the partners or consortium members.

24.5. Bidder of foreign origin may submit the Integrity Pact on its company's letterhead, duly signed by the person signing the bid.

24.6. The 'Integrity Pact' shall be submitted by the Bidder duly signed in all pages along with the Bid. The original copies shall be submitted to RailTel Office (as mentioned in this Tender document) in a separate envelope, duly superscripted with 'Integrity Pact' before due date and time of bid submission. Bid received without signed copy of the Integrity Pact document will be liable to be rejected. Format of Integrity Pact is enclosed in this Tender document.

24.7. One copy of the Integrity Pact shall be retained by RailTel and the 2nd copy will be issued to the representative of the bidders during bid opening. If the Bidder's representative is not present during the Bid opening, the 2nd copy shall be sent to the bidder by post/courier.

24.8. The Integrity Pact is applicable in this EOI/RFP vide CVC circular no. 10/05/09 dt. 18.05.09 and revised guideline of CVC circular no. 015/VGL/091 dt. 13.01.17 or the latest updated from time to time shall be followed.

24.9. Interested may also refer the URL for IP Program : https://www.railtelindia.com/EOI/RFPs/integrity-pact.html .

25. Clause wise Compliance

Clause wise compliance statement of EOI/RFP terms and conditions and technical compliance (Annexure –D) shall be enclosed with the offer along with the technical literature of the material and other documents in support of relevant clauses.

26. Submission of Offers

26.1. All offers in the prescribed forms should be submitted before the time and date fixed for the receipt of the offers.

26.2. In case the schedule of requirement quoted by tenderer is incomplete with reference to tender document, the offer is liable to be rejected.

26.3. ATTESTATION OF ALTERATION: No scribbling is permissible in the tender documents. Tender containing erasures and alterations in the tender documents are liable to be rejected. Any correction made by the tenderer/ tenderers in his/their entries must be signed (not initialed) by him/them.

26.4. The tenderer shall submit his bid online using the e-Procurement Portal https://railtel.enivida.com/. For detailed instructions please refer to e-nivida Portal.

26.5. The offer shall be submitted in two packet. Both Bids Credential Bid (Techno-Commercial Bid) & Price Bid shall be online using the e-Procurement Portal https://railtel.enivida.com/ The bid shall consist of following documents:-

a) Offer Letter complete.
b) Schedule of Requirements with quantities but with prices blanked out (this will be a replica of price bid with prices blanked out).

c) Earnest Money in prescribed form.
d) Audited balance sheet duly attested by Notary Public.
e) Constitution of Firm and Power of Attorney.
f) Clause wise compliance to tender conditions.
g) Copies of purchase orders and other documents in support of meeting qualifying criteria.
h) Complete technical data and particulars of the equipment offered, as specified in the Tender papers together with descriptive literature, leaflets, Drawings, if any, complete with list etc.
i) Technical proposal of tenderer in conformity with system design or alternative proposal of the tenderer, if any.
j) System Performance Guarantee as per Form no. 2
k) Any other information desired to be submitted by the tenderer.
l) NIL Deviation certificate.

27. Constitution of Firm and power of Attorney

27.1. Any individual(s) signing the tender or other documents connected therewith should specify whether he is signing:
a) As sole proprietor of the concern or as attorney of the sole Proprietor.
b) As a partner or partners of the firm.
c) As a Director, Manager or Secretary in the case of Limited Company duly authorized by a resolution passed by the Board of Directors or in pursuance of the authority conferred by Memorandum of Association.

27.2. In the case of a firm not registered under the Indian Partnership Act, all the partners or the attorney duly authorized by all of them should sign the tender and all other connected documents. The original Power of Attorney or other documents empowering the individual or individuals to sign should be furnished to the Purchaser for verification, if required.

27.3. The RailTel will not be bound by Power of Attorney granted by the tenderer or by the changes in the composition of the firm made subsequent to the execution of the contract agreement.

27.4. In case where the Power of Attorney partnership deed has not been executed in English, the true and authenticated copies of the translation of the same by Advocate, authorized translators of Courts and Licensed Petition Writers should be supplied by the Contractor(s) while tendering for the work.

27.5. The duly notorized Power of Attorney shall be submitted online and original copy is need to be submitted by the successful bidder before issuance of LOA.

28. Opening of Bids:

28.1. Online Bids received form the Bidders shall be opened on due date and time.
28.2. RailTel shall subsequently examine and evaluate the Bids in accordance with the provisions set out in this EOI/RFP.
28.3. To facilitate evaluation of Bids, RailTel may, at its sole discretion, seek clarifications in writing from any Bidder regarding its Bid.

29. Non-Transferability & Non-Refund ability

The EOI/RFP documents are not transferable. The cost of EO document is not refundable.

30. Details of Commercial Bid / Financial Bid

30.1. Interested partner should submit commercial bid as per requirement in EOI/RFP document or subsequent corrigendum (if any).

30.2. The commercial bid should clearly bring out the cost of the services with detailed break-up of taxes.

30.3. The rates mentioned in the commercial bid of the CSP will form basis of commercial transaction between RailTel and bidder.

31. Duration of the Contract Period

The contract duration shall be same as of CUSTOMER's contract duration with RailTel until otherwise terminated earlier. Indicative contract duration is 5 (five) years from PAC, unless otherwise terminated earlier, as mentioned in this EOI/RFP document and subject to successful participation of RailTel in the pertinent CUSTOMER's EOI/RFP. The contract duration can be renewed / extended by RailTel at its discern, in case CUSTOMER extends / renews services with RailTel by virtue of extending / renewing / new issuance of one or more Purchase Order(s) placed by CUSTOMER to RailTel.

32. Restrictions on 'Transfer of Agreement'

The CSP shall not assign or transfer its right in any manner whatsoever under the contract / agreement to a third party or enter into any agreement for sub-contracting and/or partnership relating to any subject matter of the contract / agreement to any third party either in whole or in any part i.e. no sub-contracting / partnership / third party interest shall be created.

33. Suspension, Revocation or Termination of Contract / Agreement

RailTel reserves the right to suspend the operation of the contract / agreement, at any time, due to change in its own license conditions or upon directions from the competent government authorities, in such a situation, RailTel shall not be responsible for any damage or loss caused or arisen out of aforesaid action. Further, the suspension of the contract / agreement will not be a cause or ground for extension of the period of the contract / agreement and suspension period will be taken as period spent. During this period, no charges for the use of the facility of the CSP shall be payable by RailTel.

RailTel may, without prejudice to any other remedy available for the breach of any conditions of agreements, by a written notice of Three (03) month issued to the CSP, terminate/or suspend the contract / agreement under any of the following circumstances:

a) The CSP failing to perform any obligation(s) under the contract / agreement.

b) The CSP failing to rectify, within the time prescribed, any defect as may be pointed out by RailTel.

c) Non adherence to Service Level Agreements (SLA) which RailTel has committed to CUSTOMER for the pertinent EOI/RFP.

d) The CSP going into liquidation or ordered to be wound up by competent authority.

e) If the CSP is wound up or goes into liquidation, it shall immediately (and not more than a week) inform about occurrence of such event to RailTel in writing. In that case, the written notice can be modified by RailTel as deemed fit under the circumstances. RailTel may either decide to issue a termination notice or to continue the agreement by suitable modifying the conditions, as it feels fit under the circumstances.

f) It shall be the responsibility of the CSP to maintain the agreed Quality of Service, even during the period when the notice for surrender/termination of contract / agreement is pending and if the Quality of Performance of Solution is not maintained, during the said notice period, it shall be treated as material breach liable for termination at risk and consequent of which CSP's PBG related to contract

/ agreement along with PBG related to the Empanelment Agreement with RailTel shall be forfeited, without any further notice.

g) Breach of non-fulfillment of contract / agreement conditions may come to the notice of RailTel through complaints or as a result of the regular monitoring. Wherever considered appropriate RailTel may conduct an inquiry either suo-moto or on complaint to determine whether there has been any breach in compliance of the terms and conditions of the agreement by the successful bidder or not. The CSP shall extend all reasonable facilities and shall endeavor to remove the hindrance of every type upon such inquiry. In case of default by the CSP in successful implementation and thereafter maintenance of services / works as per the conditions mentioned in this EOI/RFP document, the PBG(s) of CSP available with RailTel will be forfeited.

34. Dispute Settlement

34.1. In case of any dispute concerning the contract / agreement, both the CSP and RailTel shall try to settle the same amicably through mutual discussion / negotiations. Any unsettled dispute shall be settled in terms of Indian Act of Arbitration and Conciliation 1996 or any amendment thereof. Place of Arbitration shall be New Delhi.

34.2. The arbitral tribunal shall consist of the Sole Arbitrator. The arbitrator shall be appointed by the Chairman & Managing Director (CMD) of RailTel Corporation of India Ltd.

34.3. All arbitration proceedings shall be conducted in English.

35. Governing Laws

The contract shall be interpreted in accordance with the laws of India. The courts at New Delhi shall have exclusive jurisdiction to entertain and try all matters arising out of this contract.

36. Statutory Compliance

36.1. During the tenure of this Contract nothing shall be done by CSP in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof and shall keep RailTel indemnified in this regard.

36.2. The Bidder shall comply and ensure strict compliance by his/her employees and agents of all applicable Central, State, Municipal and Local laws and Regulations and undertake to indemnify RailTel, from and against all levies, damages, penalties and payments whatsoever as may be imposed by reason of any breach or violation of any law, rule, including but not limited to the claims against RailTel or its Customer under Employees Compensation Act, 1923, The Employees Provident Fund and Miscellaneous Provisions Act, 1952, The Contract Labour (Abolition and Regulation) Act 1970, Factories Act, 1948, Minimum Wages Act and Regulations, Shop and Establishment Act and Labour Laws which would be amended/modified or any new act if it comes in force whatsoever, and all actions claim and demand arising therefrom and/or related thereto.

37. Updation of Labour Data on Indian Railway's Shramik Kalyan Portal

Contractor is to abide by the provisions of Payment of Wages Act & Minimum Wages Act in terms of clause 54 and 55 of Indian Railways General Condition of Contract. In order to ensure the same, an application has been developed and hosted on website 'www.shramikkalyan.indianrailways.gov.in'. Contractor shall register his firm/company etc. and upload requisite details of labour and their payment in

this portal. These details shall be available in public domain. The Registration/updation of Portal shall be done as under:

(a) Contractor shall apply for one-time registration of his company/firm etc. in the Shramik Kalyan portal with requisite details subsequent to issue of Letter of Acceptance. Engineer shall approve the contractor's registration on the portal within 7 days of receipt of such request.

(b) Contractor once approved by any Engineer, can create password with login ID (PAN No.) for subsequent use of portal for all LOAs issued in his favour.

(c) The contractor once registered on the portal, shall provide details of his Letter of Acceptance (LoA)/Contract Agreements on Shramik Kalyan portal within 15 days of issue of any LoA for approval of concerned engineer. Engineer shall update (if required) and approve the details of LoA filled by contractor within 7 days of receipt of such request.

(d) After approval of LOA by Engineer, contractor shall fill the salient details of contract labours engaged in the contract and ensure updating of each wage payment to them on Shramik Kalyan portal on monthly basis.

(e) It shall be mandatory upon the contractor to ensure correct and prompt uploading of all salient details of engaged contractual labour & payments made thereof after each wage period.

(f) While processing payment of any 'On Account bill' or 'Final bill' or release of 'Advances' or 'Performance Guarantee / Security deposit', contractor shall submit a certificate to the Engineer or Engineer's representatives that "I have uploaded the correct details of contract labours engaged in connection with this contract and payments made to them during the wage period in Railway's Shramikkalyan portal at 'www.shramikkalyan.indianrailways.gov.in' till _____Month, _____Year."

38. Intellectual Property Rights

38.1. Each party i.e. RailTel and CSP, acknowledges and agree that the other party retains exclusive ownership and rights in its trade secrets, inventions, copyrights, and other intellectual property and any hardware provided by such party in relation to this contract / agreement.

38.2. Neither party shall remove or misuse or modify any copyright, trade mark or any other proprietary right of the other party which is known by virtue of this Tender and subsequent contract in any circumstances.

39. Severability

In the event any provision of this EOI/RFP and subsequent contract with CSP is held invalid or not enforceable by a court of competent jurisdiction, such provision shall be considered separately and such determination shall not invalidate the other provisions of the contract and Annexure/s which will be in full force and effect.

40. Force Majeure

40.1. If during the contract period, the performance in whole or in part, by other party, of any obligation under this is prevented or delayed by reason beyond the control of the parties including war, hostility, acts of the public enemy, civic commotion, sabotage, Act of State or direction from Statutory Authority, explosion, epidemic, quarantine restriction, strikes and lockouts (as are not limited to the establishments and facilities of the parties), fire, floods, earthquakes, natural calamities or any act of GOD (hereinafter referred to as EVENT) , provided notice of happenings of any such event is given by the affected party to the other, within twenty one (21) days from the date of occurrence thereof, neither party shall have any such claims for damages against the other, in respect of such non-performance or delay in performance. Provided service under this contract shall be resumed as soon as practicable, after such EVENT comes to an end or ceases to exist.

40.2. In the event of a Force Majeure, the affected party will be excused from performance during the existence of the force Majeure. When a Force Majeure occurs, the affected party after notifying the other party will attempt to mitigate the effect of the Force Majeure as much as possible. If such delaying cause shall continue for more than sixty (60) days from the date of the notice stated above, the party injured by the inability of the other to perform shall have the right, upon written notice of thirty (30) days to the other party, to terminate this contract. Neither party shall be liable for any breach, claims, and damages against the other, in respect of non-performance or delay in performance as a result of Force Majeure leading to such termination.

41. Indemnity

41.1. The CSP agrees to indemnify and hold harmless RailTel, its officers, employees and agents (each an "Indemnified Party") promptly upon demand at any time and from time to time, from and against any and all losses, claims, damages, liabilities, costs (including reasonable attorney's fees and disbursements) and expenses (collectively, "Losses") to which the Indemnified party may become subject, in so far as such losses directly arise out of, in any way relate to, or result from :

a) Any mis-statement or any breach of any representation or warranty made by CSP or

b) The failure by the CSP to fulfill any covenant or condition contained in this contract by any employee or agent of the Bidder. Against all losses or damages arising from claims by third Parties that any Deliverables (or the access, use or other rights thereto), created by CSP pursuant to this contract, or any equipment, software, information, methods of operation or other intellectual property created by CSP pursuant to this contract, or the SLAs (i) infringes a copyright, trade mark, trade design enforceable in India, (ii) infringes a patent issues in India, or (iii) constitutes misappropriation or unlawful disclosure or used of another Party's trade secrets under the laws of India (collectively, "Infringement Claims"); or

c) Any compensation / claim or proceeding by any third party against RailTel arising out of any act, deed or omission by the CSP or

d) Claim filed by a workman or employee engaged by the CSP for carrying out work related to this agreement. For the avoidance of doubt, indemnification of Losses pursuant to this section shall be made in an amount or amounts sufficient to restore each of the Indemnified Party to the financial position it would have been in had the losses not occurred.

41.2. Any payment made under this contract to an indemnity or claim for breach of any provision of this contract shall include applicable taxes.

42. Limitation of Liability towards RailTel

42.1. The CSP liability under the contract shall be determined as per the Law in force for the time being. The CSP shall be liable to RailTel for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the CSP and its employees (direct or indirect), including loss caused to RailTel on account of defect in goods or deficiency in services on the part of CSP or his agents or any person / persons claiming through under said CSP, However, such liability of the CSP shall not exceed the total value of the contract.

42.2. This limit shall not apply to damages for bodily injury (including death) and damage to real estate property and tangible personal property for which the CSP is legally liable.

42.3. In case of any liability/penalty imposed by RailTel Customer to RailTel, same shall be passed on to selected bidder.

43. Confidentiality cum Non-disclosure

43.1. The Receiving Party agrees that it will not disclose to third party/parties any information belonging to the Disclosing Party which is provided to it by the Disclosing Party before, during and after the execution of this contract. All such information belonging to the Disclosing Party and provided to the Receiving Party shall be considered Confidential Information. Confidential Information includes prices, quotations, negotiated issues made before the execution of the contract, design and other related information. All information provided by Disclosing Party to the Receiving Party shall be considered confidential even if it is not conspicuously marked as confidential.

43.2. Notwithstanding the foregoing, neither Party shall have any obligations regarding non-use or non-disclosure of any confidential information which:

a) Is already known to the receiving Party at the time of disclosure:

b) Is or becomes part of the public domain without violation of the terms hereof;

c) Is shown by conclusive documentary evidence to have been developed independently by the Receiving Party without violation of the terms hereof:

d) Is received from a third party without similar restrictions and without violation of this or a similar contract.

43.3. The terms and conditions of this contract, and all annexes, attachments and amendments hereto and thereto shall be considered Confidential Information. No news release, public announcement, advertisement or publicity concerning this contract and/or its contents herein shall be made by either Party without the prior written approval of the other Party unless such disclosure or public announcement is required by applicable law.

43.4. Notwithstanding the above, information may be transmitted to governmental, judicial, regulatory authorities, if so, required by law. In such an event, the Disclosing Party shall inform the other party about the same within 30 (thirty) Days of such disclosure.

43.5. This Confidentiality and Non- Disclosure clause shall survive even after the expiry or termination of this contract.

44. Assignment

Neither this contract nor any of the rights, interests or obligations under this contract shall be assigned, in whole or in part, by operation of law or otherwise by any of the Parties without the

prior written consent of each of the other Parties. Any purported assignment without such consent shall be void. Subject to the preceding sentences, this contract will be binding upon, inure to the benefit of, and be enforceable by, the Parties and their respective successors and assigns.

45. Insurance

The CSP agrees to take insurances to cover all the elements of the project under this EOI/RFP including but not limited to Manpower, Hardware, Software etc..

46. Exit Management

46.1. Exit Management Purpose

a) This clause sets out the provision, which will apply during Exit Management period. The parties shall ensure that their respective associated entities carry out their respective obligation set out in this Exit Management Clause.

b) The exit management period starts, in case of expiry of contract, at least 03 months prior to the date when the contract comes to an end or in case of termination contract, on the date when the notice of termination is sent to the CSP. The exit management period ends on the date agreed upon by RailTel or Three (03) months after the beginning of the exit management period, whichever is earlier.

46.2. Confidential Information, Security and Data : CSP will promptly, on the commencement of the exit management period, supply to RailTel or its nominated agencies the following *(if asked by RailTel in writing)*:

a) Information relating to the current services rendered and performance data relating to the performance of the services; documentation relating to the project, project's customized source code *(if any)*; any other data and confidential information created as part of or is related to this contract;

b) All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable RailTel and its nominated agencies, or its replacing vendor to carry out due diligence in order to transition the provision of the services to RailTel or its nominated agencies, or its replacing vendor (as the case may be).

46.3. Employees: Promptly on reasonable request at any time during the exit management period, the CSP shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide RailTel a list of all employees (with job titles and communication address), dedicated to providing the services at the commencement of the exit management period; To the extent that any Transfer Regulation does not apply to any employee of the CSP, RailTel or the replacing vendor may make an offer of contract for services to such employees of the CSP and the CSP shall not enforce or impose any contractual provision that would prevent any such employee from being hired by RailTel or any replacing vendor.

46.4. Rights of Access to Information : Besides during the contract period, during the exit management period also, if asked by RailTel in writing, the CSP shall be obliged to provide an access of information to RailTel and / or any Replacing Vendor in order to make an inventory of the Assets (including hardware / software / active / passive), documentations, manuals, catalogues, archive data, Live data, policy documents or any other related material.

Note: RailTel at its sole discern may not enforce any or all clauses / sub-clauses under the 'Exit Management' clause due to administrative convenience or any other reasons as deemed fit by RailTel.

47. Waiver

Except as otherwise specifically provided in the contract, no failure to exercise or delay in exercising, any right, power or privilege set forth in the contract will operate as a waiver of any right, power or privilege.

48. Changes in Contract Agreement

No modification of the terms and conditions of the Contract Agreement shall be made except by written amendments signed by the both CSP and RailTel.

49. INSTALLATION, TESTING & COMMISSIONING

49.1. Installation, Configuration and Commissioning: Bidders must complete the installation of all the supplied solution at Customer location within 6 months from date of award of contract by RailTel.

49.2. PROVISIONAL ACCEPTANCE CERTIFICATE (PAC)

On Installation, Configuration and Commissioning of supplied solution in each building of EDUCATION UNIVERSITY, the bidder shall certify and advise RailTel Supervisor where solution has been deployed, in writing that the installation is (i) completed (ii) ready for satisfactory commercial service and (iii) ready to be handed over. After successful completion of Site Acceptance Testing, a report (SAT) shall be forwarded to RailTel competent Authority. Provisional Acceptance Certificate (PAC) on completion of each building work will be issued by RailTel competent Authority. PAC will not be held back for want of minor deficiencies not affecting the functioning of the solution. Deficiencies, if any, pointed at the time of issuance of PAC, will be rectified by the contractor within one month.

49.3. FINAL ACCEPTANCE CERTIFICATE (FAC)

The final acceptance of the works completed shall take effect from the date of successful completion of 1 year warranty period after issue of last PAC provided in any case that the contractor has complied fully with his obligations in respect of each item under the contract. The Final Acceptance Certificate against the contract shall be issued by RailTel competent Authority. Notwithstanding the issue of Final Acceptance Certificate, the contractor and the purchaser shall remain liable for fulfillment of any obligation incurred under the provision of the contract prior to the issue of Final Acceptance Certificate which remains unperformed at the time such certificate is issued and for determining the nature and extent of such obligation the contract shall be deemed to remain in force between the parties hereto.

49.4. 4 years O&M period after FAC

On issuance of FAC, O&M period of 4 years duration shall start in which the selected bidder shall responsible for operations and maintenance of deployed solution in all buildings. The selected bidder shall deploy minimum 5 on-site resource L2/L3 for satisfactory O&M services. Bidder has to submit the operation and maintenance plan during technical presentation.

E-tendering Instructions to Bidders

50. INSTRUCTIONS FOR ONLINE BID SUBMISSION:

Following are the instruction for online bid submission as per the term and conditions:

The bidders are required to submit soft copies of their bids electronically on the e-tender Portal, using valid Class 3 Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the e-tender Portal and submitting their bid online on the e-tendering portal as per uploaded bid. **Prepare their bids in accordance with the requirements and submitting their bids online on the e-tender Portal.**

More information useful for submitting online bids on the e-tender Portal may be obtained at: **https://railtel.enivida.com.**

51. REGISTRATION:

i. Bidders are required to enroll on the e-Procurement Portal (URL: **https://railtel.enivida.com**) by clicking on the link "Online bidder Registration" on the e-tender Portal by paying requisite Registration fee as mentioned on the e-portal (Approx Rs.2360/-) Per vendor/per year.

ii. As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.

iii. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication with the bidder.

iv. Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate **(Only Class III Certificates with signing + encryption key usage)** issued by any Certifying Authority recognized by CCA India (e.g. Sify / TCS / nCode / eMudhra etc.), with their profile.

v. 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 DSC's to others which may lead to misuse.

vi. 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.

vii. The scanned copies of all original documents should be uploaded in pdf format on portal https://railtel.enivida.com.

viii. After completion of registration payment, you need to send your acknowledgement copy on our help desk e-mail id ewizardhelpdesk@gmail.com for activation of your account.

52. SEARCHING FOR TENDER DOCUMENTS

i. There are various search options built in the RailTel Corporation of India Limited e-tender Portal, to facilitate bidders to search active tenders by several parameters.

ii. Once the bidders have selected the tenders they are interested, they can pay the processing fee as mentioned on the e-portal (Including GST) (NOT REFUNDABLE) by net-banking / Debit / Credit card. After that respective contractor/Vendor may download the required documents / tender schedules, Bid documents etc. Once you pay both fee tenders will be moved to the respective 'requested' Tab. This would enable the e- tender Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.

53. PREPARATION OF BIDS

1. Bidder should take into account any corrigendum published on the tender document before submitting their bids.

2. Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.

3. 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 formats. Bid Original documents may be scanned with 100 dpi with colored option which helps in reducing size of the scanned document.

4. To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use "My Documents" available to them to upload such documents.

5. These documents may be directly submitted from the "My Documents" area while submitting a bid and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process.

54. SUBMISSION OF BIDS

1. Bidder should log into the website well in advance for the submission of the bid so that it gets uploaded well in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to any issues.

2. The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document as a token of acceptance of the terms and conditions laid down by RailTel.

3. Bidder has to select the payment option as "Online Payment" to pay the tender fee / EMD as applicable and enter details of the instrument.

4. Bidder should submit the EMD online as per the instructions specified in the tender document. In case of non-submission of EMD amount (where applicable) online, the uploaded bid will be summarily rejected.

5. Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BOQ format with the tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BOQ file, open it and complete the white Colored (unprotected) cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BOQ file is found to be modified by the bidder, the bid will be rejected.

6. 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, opening of bids etc. The bidders should follow this time during bid submission.

7. All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data. The data entered cannot be viewed by unauthorized persons until the time of bid opening. Data storage encryption of sensitive fields is done. Any bid document that is uploaded to the server is subjected to symmetric encryption using a system generated symmetric key. Further this key is subjected to asymmetric encryption using buyers/bid opener public keys. Overall, the uploaded tender documents become readable only after the tender opening by the authorized bid openers.

8. The uploaded tender documents become readable only after the tender opening by the authorized bid openers.

9. Upon the successful and timely submission of bid click "Complete" (i.e. after Clicking "Submit" in

the portal), the portal will give a successful Tender submission acknowledgement & a bid summary will be displayed with the unique id and date & time of submission of the bid with all other relevant details.

10. The tender summary has to be printed and kept as an acknowledgement of the submission of the tender. This acknowledgement may be used as an entry pass for any bid opening meetings.

55. ASSISTANCE TO BIDDERS:

1. 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.

2. Any queries relating to the process of online bid submission or queries relating to e-tender Portal in general may be directed to the 24x7 Helpdesk Support.

   Please feel free to contact RailTel E-Nivida Helpdesk (as given below) for any query related to e-tendering.

   i. Helpdesk landline No: 011-49606060

   ii. Mr. Amrendra (8448288980)

   iii. Mr. Birendra Kumar (8448288988)

   RailTel Contact-I (for general Information)
   Ashutosh Gupta: Mgr/DC
   Telephone 0124-2714000
   E-mail ID: ashutosh.gupta@railtelindia.com

   RailTel Contact-II (for general Information)

   Rajeev Kumar: DGM/ITP
   Telephone 0124-2714000
   E-mail ID: rajeevkumar@railtelindia.com

56. BID RELATED INFORMATION FOR THIS TENDER

The entire bid-submission would be online on RailTel E-Nivida Portal.
Broad outline of submissions are as follows:

i. Submission of Bid Security/ Earnest Money Deposit (EMD)
ii. Submission of digitally signed copy of Tender Documents/Addenda
iii. Two Packet
iv. Online response to Terms & Conditions of Tender.
v. (Optional) Online Submission of modification, substitution bids for technical or financial parts, or withdrawal bid.

NOTE: Bidder must ensure that the bid must be successfully submitted online as per instructions of RailTel E-Nivida Portal.

57. ONLINE SUBMISSIONS

The bidder is required to submit all the relevant documents online only with the following documents.

a) EMD submission as per details mentioned in tender notice.

b) Tender Cost submission as per details mentioned in tender notice.

c) Power of attorney to be submitted online in accordance with Clause – 34, Chapter 6 Original copy is needed to be submitted by the successful bidder before issuance of LOA.

d) In case bidder happens to be an MSE bidder, the documentary evidence for same shall be submitted on line.

58. SUBMISSION OF ELIGIBILITY CRITERIA RELATED DOCUMENTS:

Eligibility criteria related documents as applicable shall also be scanned and submitted "ONLINE"

NOTE: In case of internet related problem at a bidder's end, especially during 'critical events' such as a short period before bid-submission deadline, during online public tender opening event, during e-auction, it is the bidder's responsibility to have backup internet connections.
In case there is a problem at the e-procurement/ e-auction service provider's end (in the server, leased line, etc.) due to which all the bidders face a problem during critical events, and this is brought to the notice of RailTel by the bidders in time, then RailTel will promptly reschedule the affected event(s).

59. INSTRUCTIONS FOR TENDER DOCUMENT TO THE BIDDERS:

The RailTel Tenders are published on www.railtelindia.com and on RAILTEL E-NIVIDA Portal https://railtel.enivida.com/.

NOTE: For online bid submission the bidder will have to necessarily download an official online copy of the tender documents from RAILTEL E-NIVIDA portal, and this should be done well before the deadline for bid-submission.

60. SUBMISSION OF OFFERS AND FILLING OF TENDER:

This e-tender should be duly submitted online using the e-Procurement Portal https://railtel.enivida.com/. For detailed instructions please refer to RAILTEL E-NIVIDA Portal.

61. ATTENDANCE OF REPRESENTATIVES FOR TENDER OPENING:

Representatives of bidders desirous to attend the tender opening can do so on production of a proper letter of authority from the respective firm, failing which they may not be allowed to attend the tender opening. Authorized representatives of those firms who have submitted the tender documents alone shall be allowed to attend the tender opening.

Annexure - 01

EOI/RFP COVER LETTER

(On Organization Letter Head)

Bid Ref No. :

Date:

To,

General Manager (ITP),
RailTel Corporation of India Limited,
Plate-A, 6th Floor, Office Block Tower-2,
East Kidwai Nagar, New Delhi - 110023

Ref : EOI/RFP No. RCIL/EOI/RFP/CO/ITP/2022-23/ IT services to RCIL Customer/10

Dear Sir/Ma'm,

1. I, the undersigned, on behalf of M/s ……., having carefully examined the referred EOI/RFP offer to participate in the same, in full conformity with the said EOI/RFP and all the terms and conditions thereof, including corrigendum issued till last date of submission of EOI/RFP.

2. I agree to abide by this Proposal, consisting of this letter, our Pre-qualification, Technical and Commercial Proposals *(at subsequent stage)*, for a period of 120 days from the date fixed for submission of Proposals as stipulated in the EOI/RFP and modifications resulting from contract negotiations, and it shall remain binding upon us and may be accepted by you at any time before the expiration of that period.

3. I acknowledge that the Authority will be relying on the information provided in the Proposal and the documents accompanying the Proposal for selection of the Commercially Suitable Partner (CSP) for the aforesaid Service, and we certify that all information provided therein is true and correct; nothing has been omitted which renders such information misleading; and all documents accompanying the Proposal are true copies of their respective originals.

4. I undertake, if our Bid is accepted, to commence our services as per scope of work as specified in the contract document.

5. Until a formal Purchase Order or Contract is prepared and executed, this Bid and supplement / additional documents submitted (if any), together with your written acceptance thereof in your notification of award shall constitute a binding contract between us.

Signature of Authorised Signatory

Name
Designation

Annexure – 02

Compliance to Rule 144 (xi) of GFR, 2017 ***including amendments till date***
(On Organization Letter Head)

Bid Ref No. :

Date:

To,

General Manager (ITP),
RailTel Corporation of India Limited,
Plate-A, 6th Floor, Office Block Tower-2,
East Kidwai Nagar, New Delhi - 110023

Ref : EOI/RFP No. RCIL/EOI/RFP/CO/ITP/2022-23/ IT services to RCIL Customer/10

Dear Sir/Ma'm,

I, the undersigned, on behalf of M/s ……. , have read the clause/para regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries.

(a) I certify that M/s ……. is not from such a country and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I also certify that M/s …… will not offer any products / services of entity from such countries unless such entity is registered with the Competent Authority.

OR *(Strikeout either (a) or (b), whichever is not applicable)*

(b) I certify that M/s …… is from such a country and has been registered with the Competent Authority. I also certify that M/s ……. has product/services of entity from such countries and these entity / entities are also registered with the Competent Authority.

(Where applicable, evidence of valid registration by the Competent Authority is to be attached with the bid.)

I hereby certify that M/s …… fulfills all requirements in this regard and is eligible to be considered.

I hereby acknowledge that in the event of acceptance of my bid on above certificate and if the certificate is found to be false at any stage, the false certificate would be a ground for immediate termination of contract and further legal action in accordance with the Law.

Signature of Authorised Signatory

Name
Designation

Annexure - 03

Local Content Compliance

(On Organization Letter Head or On Letter Head of Statutory Auditor / Cost Auditor*)*

Bid Ref No. :

Date:

To,

General Manager (ITP),
RailTel Corporation of India Limited,
Plate-A, 6th Floor, Office Block Tower-2,
East Kidwai Nagar, New Delhi - 110023

Ref : EOI/RFP No. RCIL/EOI/RFP/CO/ITP/2022-23/ IT services to RCIL Customer/10

Dear Sir/Ma'm,

I, the undersigned, on behalf of M/s ……. , hereby submits that our technical solution for the 'Scope of Work' mentioned under the EOI/RFP document is in compliance of local content requirement and makes us equivalent to 'Class-I local supplier' / 'Class-II local supplier' *(mention whichever is applicable)* for the Tender under reference, as defined under the order No. P-45021/2/2017-PP(BE-II) dt. 04-June-2020 issued by Ministry of Commerce and Industry, Govt. of India.

I hereby certify that M/s …… fulfills all requirements in this regard and is eligible to be considered and for the submitted bid Local Content Percentage is …….. % *(write in figures as well as in words).*

I hereby acknowledge that in the event of acceptance of bid of M/s …….. on above certificate and if the certificate is found to be false at any stage, the false certificate would be a ground for immediate termination of contract and further legal action in accordance with the Law, including but not limited to the encashment of Bank Guarantee related to Empanelment and Performance Bank Guarantee (PBG), as available with RailTel, related to this Tender.

Signature of Authorised Signatory

Name
Designation

**To be signed by Statutory Auditor / Cost Auditor in case bid value is exceeding INR 10 Crores.*

Annexure – 04

Undertaking for Non-Blacklisting, Arbitration Case, Absence of Conflict of Interest

(On Organization Letter Head)

Bid Ref No. :

Date:

To,

General Manager (ITP),
RailTel Corporation of India Limited,
Plate-A, 6th Floor, Office Block Tower-2,
East Kidwai Nagar, New Delhi - 110023

Ref : EOI/RFP No. RCIL/EOI/RFP/CO/ITP/2022-23/ IT services to RCIL Customer/10

Dear Sir/Ma'm,

I, the undersigned, on behalf of M/s ……..……. , hereby submits that

1. We are not blacklisted by any State / Central Government Ministry / Department / Corporation / Autonomous Body at the time of submission of bid.
2. We are not having any ongoing or past, arbitration case(s) with RailTel or CUSTOMER or Organizations under Indian Railways, at the time of submission of bid.
3. We are not in position of conflict-of-interest (as defined in the EOI/RFP document) at the time of submission of bid.

I hereby acknowledge that in the event of acceptance of bid of M/s …….. on above undertaking and if the undertaking is found to be false at any stage, the false undertaking would be a ground for immediate termination of contract and further legal action in accordance with the Law, including but not limited to the encashment of Bank Guarantee related to Empanelment and Performance Bank Guarantee (PBG), as available with RailTel, related to this Tender.

Signature of Authorised Signatory

Name
Designation

Annexure – 05

PROFORMA FOR SIGNING THE INTEGRITY PACT

(On Stamp paper of Appropriate Value)

RailTel Corporation of India Limited, hereinafter referred to as "The Principal".

And

……., hereinafter referred to as "The Bidder/ Contractor"

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for …….. . The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fair- ness/transparency in its relations with its Bidder(s) and /or Contractor(s).

In order to achieve these goals, the Principal will appoint an Independent External Monitor (IEM), who will monitor the EOI/RFP process and the execution of the contract for compliance with the principles mentioned above.

Section 1- Commitments of the Principal

1. 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 EOI/RFP for, or the execution of a 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 EOI/RFP process treat all Bidder(s) with equity and reason.
The Principal will in particular, before and during the EOI/RFP 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 process or the contract execution.

c. The Principal will exclude from the process all known prejudiced persons.

2. If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the 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 actions.

Section 2- Commitments of the Bidder(s) /Contractor(s)

1. The Bidder(s)/Contractor(s) commit himself to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the EOI/RFP process and during the contract execution.

a. The Bidder(s)/contractor(s) will not, directly or through any other persons or firm, offer promise or give to any of the Principal's employees involved in the EOI/RFP 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 ad- vantage during EOI/RFP process or during the execution of the contract.

b. The Bidder(s)/Contractor(s) will not enter with other Bidders 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 the relevant IPC/PC Act; further the Bidder(s) /Contractors will not use improperly, for purposes of com- petition or personal gain, or pass on to 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)/Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract. Further, details as mentioned in the "Guidelines on Indian Agent of Foreign Suppliers" shall be disclosed by the Bidder(s) / Contractor(s). Further, as

mentioned in the Guidelines all the payments made to the Indian agent / representative have to be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers" as annexed and marked as Annexure-A.

2. The Bidder(s)/Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3: Disqualification from EOI/RFP process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a 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 the Bidder(s)/Contractor(s) from the EOI/RFP process or take action as per the procedure mentioned in the "Guidelines on banning of business dealings". Copy of the "Guidelines on Banning of Business Dealings" is annexed and marked as Annexure-B.

Section 4: Compensation for Damages

1. If the Principal has disqualified the Bidder(s) from the EOI/RFP process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/Bid Security.

2. If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to be terminated the contract according to Section 3, the Principal shall be en-titled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5: Previous Transgression

1. The Bidder declares that no previous transgressions occurred in the last three years with any other company in any country conforming to the anti-corruption approach or with any other public sector enterprise in India that could justify his exclusion from the EOI/RFP process.

2. If the bidder makes incorrect statement on this subject, he can be disqualified from the EOI/RFP process for action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6: Equal treatment of all Bidders/ Contractors/Subcontractors

1. The Bidder(s)/Contractor(s) undertake(s) to demand from all subcontractors a commitment in conformity with this Integrity Pact, and to submit it to the Principal before contract signing.

2. The Principal will enter into agreements with identical conditions as this one with all bidders, contractors and subcontractors.

3. The Principal will disqualify from the EOI/RFP process all bidders who do not sign this Pact or violate its provisions.

Section 7: Criminal charges against violation by Bidder(s) / Contractor(s) / Sub Contractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8: Independent External Monitor / Monitors

1. The Principal appoints competent and credible Independent External Monitor 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 agreement.

2. The Monitor is not subject to instructions by the representatives of the parties and per- forms his functions neutrally and independently. He reports to the CMD, RailTel.

3. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all project documentation of the Principal including that provided by the Con- tractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/Subcontractor(s) with confidentiality.

4. The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

5. 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 a specific manner, refrain from action or tolerate action.

6. The Monitor will submit a written report to the CMD, RailTel within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

7. Monitor shall be entitled to compensation on the same terms as being extended to provided to Independent Directors on the RailTel Board.

8. If the Monitor has reported to the CMD, RailTel, a substantiated suspicion of an offence under relevant IPC/PC Act, and the CMD, RailTel 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.

9. The word 'Monitor' would include both singular and plural.

Section 9: Pact Duration

This pact begins when both parties have legally signed it. It expires for the Contractor 10 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded.

If any claim is made / lodged by either party during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by CMD of RailTel.

Section 10: Other Provisions

1. This agreement is subject to Indian Law, Place of performance and jurisdiction is the Registered Office of the Principal, i.e. New Delhi.

2. Changes and supplements as well as termination notices need to be made in writing.

3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

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

(For & On behalf of the Principal)
(Office Seal)

Place ——————
Date ——————

(For & On behalf of Bidder/Contractor)
(Office Seal)

Place ——————
Date ——————

Witness 1: _____

(Name & Address) _____

Witness 2: _____

(Name & Address) _____

Annexure – 06

Commercial Bid

(On Organization Letter Head)

Bid Ref No. :

Date:

To,

General Manager (ITP),
RailTel Corporation of India Limited,
Plate-A, 6th Floor, Office Block Tower-2,
East Kidwai Nagar, New Delhi - 110023

Ref : EOI/RFP No. RCIL/EOI/RFP/CO/ITP/2022-23/ IT services to RCIL Customer/10

Financial BID				
E-EOI/RFP No. :- RCIL/EOI/RFP/CO/ITP/2022-23/ IT services to RCIL Customer/10				
Name of Work:- RFP for Selection of Partner for work of "Implementation of State-of-the-Art ICT Infrastructure on turnkey basis at University Campus in New Delhi"				
all below boxes in SKY BLUE needs to be mandatorily filled				
Name of the Company/Firm				
Sl.No.	**Item Category**	**Total Amount**	**GST**	**Total Amount including GST**
A	Camera			0.00
B	IT infrastructure and associated items at LS, ES, Admin, Data Centre			0.00
C	Networking Devices for Campus and Buildings			0.00
D	Applications, Licenses and Solution Proposed at Data Centre			0.00
E	Non IT components for ICCC			0.00
F	Passive Material at Back Bone Connectivity			0.00
	Total Capex			0.00
	Total Opex (for deployment of O&M Manpower at customer location for the period of 4 years from date of issue of FAC)			0.00
	Sub Total SOR (Capex+ Opex)			0.00

SOR Item wise detail:

SN	Description	Unit	Estimated Qty	Unit Price (Included Warranty)	Total Price (without GST)	GST %	GST Amount	Total Amount including GST
A	**IP cameras**							
1	SITC of Full HD Fixed dome type IP colour camera along with all accessories and 128 GB Class 10 SD Card	Nos	1307					
2	SITC of Full HD Bullet type IP colour camera along with all accessories and and 128 GB Class 10 SD Card	Nos	116					
3	SITC of Full HD P/T/Z type IP colour camera along with all accessories and 128 GB Class 10 SD Card	Nos	41					
4	SITC of Digital Key-Board (Joystick) compatible with PTZ cameras along with all accessories	Nos	12					
5	SITC of 4K UHD Bullet type IP colour camera along with all accessories and 128 GB Class 10 SD Card (FRS)	Nos	10					
6	SITC of Fixed Box IP colour camera along with all accessories and 128 GB Class 10 SD Card (ANPR)	Nos	6					
B	**IT infrastructure and associated items at LS, ES, Admin, Data Centre**							
1	SITC of Server for Video Management system	Nos	2					
2	SITC of Video Recording with N+1 redundancy along with all accessories	Nos	14					
3	SITC of Server for Video Analytics along with all accessories	Nos	2					
4	SITC of Server for Facial Recognition System along with all accessories	Nos	1					
5	SITC of Server for EMS System along with all accessories	Nos	3					
6	SITC of Server for ICCC Application along with all accessories	Nos	3					
7	SITC of Server/Workstation for Visitor Management System and	Nos	1					
8	SITC of Server/Workstation for Baggage Scanner System along with all accessories	Nos	1					

9	SITC of Server/Workstation for Backup Solution along with all accessories	Nos	1					
10	SITC of PC Workstation for viewing, monitoring and system management including 2 Nos 4K UHD 24" LED Monitor	Nos	17					
11	SITC of Storage System at Data Centre with 30 days recording with backup Solution	Lot	1					
C	**Networking Devices for Campus and Buildings**							
1	SITC of Access switch 16 Port Non POE along with all accessories	Nos	15					
2	SITC of Access switch 24 Port Non POE along with all accessories	Nos	20					
3	SITC of Access switch 48 Port Non POE along with all accessories	Nos	115					
4	SITC of Industrial Grade 8 Port POE+ Switch along with all accessories for Perimeter Boundary	Nos	40					
5	SITC of Distribution Switch for Perimeter Boundary along with all accessories	Nos	12					
6	SITC of Access switch 16 - PoE+ along with all accessories	Nos	46					
7	SITC of Access switch 24 - PoE +along with all accessories	Nos	95					
8	SITC of Access switch 48 - PoE + along with all accessories	Nos	65					
9	SITC of Distribution Switch 48 Port along with all accessories	Nos	20					
10	SITC of Core Switch along with all accessories	Nos	2					
11	SITC of Wi-Fi Access Point - Indoor along with all accessories Price to be quoted after Considering the clause/Note mentioned in Annexure-C (For wi-fi Products under cluse 1.1.1)	Nos	868					
12	SITC of Wi-Fi Access Point - Outdoor along with all accessories	Nos	30					
13	SITC of Wi-Fi- Controller along with all accessories. Price to be quoted after Considering the clause/Note mentioned in Annexure-C (For wi-fi Products under cluse 1.1.1)	Nos	2					
14	SITC of Router along with all accessories	Nos	2					

15	SITC of Network Access Controller (NAC) along with all accessories	Nos	2					
16	SITC of SAN Switch along with all accessories	Nos	2					
17	SITC of WAF along with all accessories	Nos	2					
18	Spares @ 5% of supply against item Cameras, Switches (Access and Distribution), Wi-Fi Access Points	Lot	1					
D	**Applications, Licenses and Solution Proposed at Data Centre**							
1	SITC of Software (including bases license and per camera basis) for Video Management and Video recording	Lot	1					
2	SITC of Software (including bases license and per camera basis) for Facial Recognition System	Lot	1					
3	SITC of Software (including bases license and per camera basis) for ICCC	Lot	1					
4	SITC of Visitor Management Solution including hardware and software	Lot	1					
5	SITC of EMS Application at Data Centre	Lot	1					
6	Integration of other system with ICCC	Lot	1					
7	SITC of Single Sign ON (SSO) Application at Data Centre	Lot	1					
8	SITC of 85 Nos. Smart Class room solution includes hardware and software	Lot	1					
9	**SITC of Gate Management System**	Lot	1					
a	Boom Barrier with RFID	Nos	6					
b	Baggage Scanner	Nos	3					
10	ANPR Solution	Lot	1					
11	SITC of IPBX Solution with complete hardware and application	Lot	1					
E	**Non IT components for ICCC**							
1	2x3 Video Wall Cubes LED 70 inch Backlit Display	Lot	1					

2	Video Wall Controller with Wall Management Software	Lot	1					
3	Audio Mixer and Speaker System	Lot	1					
4	Multi Function Laser Printer	Nos	1					
5	LED Television Set (Conference Room) (55")	Nos	1					
6	Project Manager Room	Lot	1					
7	Store Room	Lot	1					
8	Air Conditioning	Lot	1					
9	150 KVA UPS with Battery backup of 30 min	Set	1					
10	Electrical and power cabling	Lot	1					
11	Lighting, WLD, Rodent Repellent as per requirement	Lot	1					
12	LAN and CAT-6 cabling	Lot	1					
13	Fire & Smoke Detection System	Lot	1					
14	Control Room Operator Desks for 12 Operators	Lot	1					
15	Conference Room for internal meeting	Nos	1					
16	Interior work with furniture for operator workstation, executive chairs, desk, etc	Lot	1					
F	**Passive Material at Back Bone Connectivity**							
1	SITC of 144 Core Multitube Single mode OS2 9/125µ. Fibre Cable	Mtrs.	8000					
2	SITC of 144 LC Fiber port Single Mode OS2 intelligent loaded LIU including pigtail etc.	Nos	4					
3	SITC of 144 Core Joint encloser	Nos	24					
4	SITC of Outdoor Street cabinet IP 55 rated for Fiber distribution point	Nos	24					
5	SITC of Fibre Patch Cord-SCAPC SCAPC, Single Mode Fiber Patch Cord, Simplex, Meet G.652.D, G.657.A1 for Cross Connectivity 3 Mtrs.	Nos	528					
6	SITC of 12 Core Single Mode OS2 9/125µ. Fibre Cable	Mtrs.	4500					
7	SITC of 24 port LC Single Mode OS2 intelligent loaded LIU including pigtail etc.	Nos	76					

8	SITC of Fibre Patch Cord- LC-LC Single Mode OS2 Patch Cord 3 Mtrs.	Nos	912					
9	SITC of 06 Core, Single mode OS2 9/125µ. Fibre cable	Mtrs.	22430					
10	SITC of 12 port LC Single mode OS2 intelligent loaded LIU including pigtail	Nos	102					
11	SITC of 12 Core OS2 SM outdoor multitube Fibre Single sheath	Mtrs.	8000					
12	SITC of 24U Outdoor distribution Cabinet with Foundation and earthing, PDB and required accessories.	Nos	6					
13	SITC of 06 Meter I-type pole with foundation with earthing & MCB provision	Nos	100					
14	SITC of 05 Meter cantilever pole with foundation with earthing with Accessories	Nos	3					
15	SITC of Surge Protection Device	Nos	140					
16	SITC of 10KVA UPS with 1hr. Backup	Nos	6					
17	SITC of Outdoor fibre splice Box	Nos	50					
18	SITC of Pole Mount Junction Box 500X400X300MM with accessories	Nos	50					
19	SITC of 3Core 2.5 Sq.mm. Copper cable outdoor rated	Mtr.	8000					
20	SITC of 3Core 10 Sq.mm. Copper cable outdoor rated	Mtr.	600					
21	SITC of 12 port LC Single mode OS2 intelligent loaded LIU including pigtail	Nos	6					
22	SITC of Cat-6 Outdoor UTP Cable	Mtr.	8000					
23	SITC of Outdoor required RJ45 Connector for Wi-Fi & CCTV Cable connect at field side	Nos	400					
24	SITC of Outdoor Faceplate with required RJ45 Jack for Wi-Fi Cable connect at field side	Nos	60					
25	SITC of Cat 6, UTP, Outdoor Copper Patch Cord	Nos	200					
26	SITC of 50MM HDPE for Fibre Cable Laying	Mtr.	10000					
27	SITC of 42U Network Rack 800X1000MM (WXD)	Nos	4					
28	SITC of 42U Server & Storage Rack 600X1200MM (WXD)	Nos	12					

29	SITC of 12-Fiber Single mode MPO12 (Pinned) to MPO12 (Pinned), Fibre Trunk Cable Assembly, Low Smoke Zero Halogen, Length 15 meter	Nos	20					
30	SITC of 12-Fiber Single mode MPO12 (Pinned) to MPO12 (Pinned), Fibre Trunk Cable Assembly, Low Smoke Zero Halogen, Length 25 meter	Nos	20					
31	SITC of 19" Rack Mount, 1U modular cassette sliding Panel, accepts 4 modules or MPO panels, providing up to 48 duplex LC ports, or up to 32 MPO ports, Single Mode	Nos	24					
32	SITC of Single mode MPO-12 Distribution Module, 1x12F MPO unpinned to 12F LC Blue, Method B Enhanced, Intelligent Ready	Nos	60					
33	SITC of Modular Panel Blank Adapter Pack, 4 Panels	Pkt	9					
34	SITC of Single mode, LC/UPC Uniboot to LC/UPC Uniboot, 2.0 mm Duplex Fibre Patch Cord, Low Smoke Zero Halogen/Riser, Length 3 meter	Nos	180					
35	SITC of Single mode, LC/UPC Uniboot to LC/UPC Uniboot, 2.0 mm Duplex Fibre Patch Cord, Low Smoke Zero Halogen/Riser, Length 5 meter	Nos	180					
36	SITC of Rack Controller for Manage the Fibre Panels	Nos	4					
37	SITC of 2U-MODULAR LC, Sliding Shelf, Upgrade Kit 5PK Kit	Nos	2					
38	SITC of 1U-MODULAR LC 5 Pack Upgrade Kit	Nos	10					
39	SITC of Rack Controller Kit/ Rack ExEOI/RFP Kit	Nos	2					
40	SITC of System Manager Enterprise 5000 Ports	Nos	1					
41	SITC of Software Assurance System Manager Enterprise 5000	Lot	1					
Total of Supply								

Note:

(1) The item quantity in above table is only estimated, however the interested bidder is required to understand the requirement and can change the quantities. In case of any shortage in quantity while implementation of solution, the selected bidder has to provide all short items without any additional cost to meet the end objective under SOR.

(2) RailTel can issue PO for partial SOR as per customer requirement.

(3) Selected bidder should submit the authorization form OEM for the items under final solution.

Signature of Authorised Signatory

Name
Designation

Form No. 1

PROFORMA FOR PERFORMANCE BANK GUARANTEE BOND
(On Stamp Paper of Rs one hundred)

(To be used by approved Scheduled Banks)

1. In consideration of the RailTel Corporation of India Limited, having its registered office at Plate-A, 6th Floor, Office Tower-2, NBCC Building, East Kidwai Nagar, New Delhi-110023 (Herein after called RailTel) having agreed to exempt ……(Hereinafter called "the said Contractor(s)") from the demand, under the terms and conditions of an Purchase Order No.……dated……made between…… and …….. for (hereinafter called " the said Agreement") of security deposit for the due fulfillment by the said Contractor (s) of the terms and conditions contained in the said Agreement, on production of a Bank Guarantee for Rs. ……(Rs …….. only). We …… (indicate the name of the Bank) hereinafter referred to as "the Bank") at the request of ……. ……. Contractor(s) do hereby undertake to pay the RailTel an amount not exceeding Rs. ……. against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor(s) of any of the terms or conditions contained in the said Agreement.

2. We, ……. Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage caused to or would be caused to or suffered by the RailTel by reason of breach by the said Contractor(s) of any of terms or conditions contained in the said Agreement or by reason of the Contractor(s) failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs . ……

3. We, …….. bank undertake to pay to the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s) / Tenderer(s) in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal. The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor(s) / Tenderer(s) shall have no claim against us for making such payment.

4. We, ……. Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the ……. …… We shall be discharged from all liability under this Guarantee thereafter.

5. We,…… (indicate the name of Bank) further agree with the RailTel that the RailTel shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for any time or from time to time any of the powers exercisable by the RailTel against the said contractor(s) and to forbear or enforce any

of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor(s) or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have affect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s) / Tenderer(s).

(indicate the name of Bank) lastly undertake not to revoke this Guarantee during its currency except with the previous consent of the RailTel in writing.

Dated the day of 2022

for ……..

(indicate the name of the Bank)

Witness

1. Signature
   Name

2. Signature
   Name

Form No. 2

PROFORMA FOR THE SYSTEM PERFORMANCE GUARANTEE
(On Stamp Paper of Rs. One hundred)

The Director,
RailTel Corporation of India Limited

I / We ……. hereby guarantee that the design on the basis of which we have submitted our EOI/RFP no. …… has been carefully made to conform to the end objectives in the EOI/RFP documents and to technical specification therein. We further guarantee that in the event of the performance of the system, when installed, not complying with the end objectives or with the specifications contained in the EOI/RFP documents, we shall provide further inputs to enable the RailTel to realize the end objectives contained in these documents without any additional payment for any additional equipment which may be required in this regard. We further guarantee that all the expenses for providing the additional inputs under the System Guarantee will be borne by us. We further guarantee that these additional inputs will be provided by us to make the system workable within 1 month from the date on which this guarantee is invoked by the Purchaser. The guarantee is valid for a period of one year from the date of commissioning of the system.

(Signature of Firm's Authorized Officer)
Seal

Signature of witness:

1. …….

2. …….

Form No. 3

FORMAT FOR AFFIDAVIT TO BE UPLOADED BY EOI/RFPER ALONGWITH THE EOI/RFP DOCUMENTS

(To be executed in presence of Public notary on non-judicial stamp paper of the value of Rs. 100/. The paper has to be in the name of the EOI/RFPer) **

I……. (Name and designation)** appointed as the attorney/authorized signatory of the EOI/RFPer (including its constituents),
M/s _____(hereinafter called the EOI/RFPer) for the purpose of the Tender documents for the work of _____ as per the EOI/RFP No. _____ of (RailTel Corporation of India Ltd.), do hereby solemnly affirm and state on the behalf of the EOI/RFPer including its constituents as under:

1. I/we the EOI/RFPer (s), am/are signing this document after carefully reading the contents.

2. I/we the EOI/RFPer(s) also accept all the conditions of the EOI/RFP and have signed all the pages in confirmation thereof.

3. I/we hereby declare that I/we have downloaded the EOI/RFP documents from RailTel website www.railtelindia.com, https://railtel.enivida.com/, I/we have verified the content of the document from the website and there is no addition, no deletion or no alternation to be content of the EOI/RFP document. In case of any discrepancy noticed at any stage i.e. evaluation of EOI/RFPs, execution of work or final payment of the contract, the master copy available with the RailTel Administration shall be final and binding upon me/us.

4. I/we declare and certify that I/we have not made any misleading or false representation in the forms, statements and attachments in proof of the qualification requirements.

5. I/we also understand that my/our offer will be evaluated based on the documents/credentials submitted along with the offer and same shall be binding upon me/us.

6. I/we declare that the information and documents submitted along with the EOI/RFP by me/us are correct and I/we are fully responsible for the correctness of the information and documents, submitted by us.

7. I/we undersigned that if the certificates regarding eligibility criteria submitted by us are found to be forged/false or incorrect at any time during process for evaluation of EOI/RFPs, it shall lead to forfeiture of the EOI/RFP EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the EOI/RFPer)** _____ and all my/our constituents understand that my/our constituents understand that my/our offer shall be summarily rejected.

8. I/we also understand that if the certificates submitted by us are found to be false/forged or incorrect at any time after the award of the contract, it will lead to termination of the contract, along with forfeiture of EMD/SD and Performance guarantee besides any other action provided in the contract including banning of business for five years on entire RailTel.

DEPONENT

SEAL AND SIGNATURE
OF THE EOI/RFPER

VERIFICATION

I/We above named EOI/RFP do hereby solemnly affirm and verify that the contents of my/our above affidavit are true and correct. Nothing has been concealed and no part of it is false.

DEPONENT

SEAL AND SIGNAURE
OF THE EOI/RFPER

Place:
Dated:

**The contents in Italics are only for guidance purpose. Details as appropriate, are to be filled in suitably by EOI/RFPer. Attestation before Magistrate/Notary Public.

FORM No.: 04

Format for Power of Attorney

POWER OF ATTORNEY

[To be executed on non-judicial stamp paper of the appropriate value in accordance with relevant Stamp Act. The stamp paper to be in the name of the company who is issuing the power of attorney.]

We, M/s._____ (name of the firm or company with address of the registered office) hereby constitute, appoint and authorise Mr. or Ms._____ (Name and residential address) who is presently employed with us and holding the position of _____, as our Attorney to do in our name and our behalf all or any of the acts, deeds or things necessary or incidental to our RFP for the Project _____ (name of the Project), including signing and submission of the RFP response, participating in the meetings, responding to queries, submission of information or documents and generally to represent us in all the dealings with Client or any other Government Agency or any person, in connection with the works until culmination of the process of bidding till the Project Agreement is entered into with _____ (Client) and thereafter till the expiry of the Project Agreement.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this power of attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us.

(Add in the case of a Consortium)
Our firm is a Member or Lead bidder of the Consortium of _____, _____ and _____.
Dated this the _____ day of _____ 2022

(Signature and Name of authorized signatory)
_____

(Signature and Name in block letters of all the remaining partners of the firm Signatory for the Company)

Seal of firm Company

Witness 1: Witness 2:

Notes:

a. To be executed by all the members individually.

b. The Mode of execution of the power of attorney should be in accordance with the procedure, if any laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.

Annexure – A

GUIDELINES FOR INDIAN AGENTS OF FOREIGN SUPPLIERS

a) There shall be compulsory registration of agents for all global (Open) Tender and Limited Tender. An agent who is not registered with RailTel Units shall apply for registration in the prescribed Application -Form.

b) Registered agents will file an authenticated Photostat copy duly attested by a Notary Public/ Original certificate of the principal confirming the agency agreement and giving the status being enjoyed by the agent and the commission/ remuneration/ retainer-ship being paid by the principal to the agent before the placement of order by RailTel.

c) Wherever the Indian representatives have communicated on behalf of their principals and the foreign parties have stated that they are not paying any commission to the Indian agents, and the Indian representative is working on the basis of salary or as retainer, a written declaration to this effect should be submitted by the party (i.e. Principal) before finalizing the order.

2.0 DISCLOSURE OF PARTICULARS OF AGENTS/ REPRESENTATIVES IN INDIA, IF ANY.

2.1 Tenderers of Foreign nationality shall furnish the following details in their offer:

2.1.1 The name and address of the agents/representatives in India, if any and the extent of authorization and authority given to commit the Principals. In case the agent/representative be a foreign Company, it shall be confirmed whether it is real substantial Company and details of the same shall be furnished.

2.1.2 The amount of commission/ remuneration included in the quoted price(s) for such agents/representatives in India.

2.1.3 Confirmation of the Tenderer that the commission/ remuneration if any, payable to his agents/ representatives in India, may be paid by RAILTEL in Indian Rupees only.

2.2 Tenderers of Indian Nationality shall furnish the following details in their offers:

2.2.1 The name and address of the foreign principals indicating their nationality as well as their status, i.e, whether manufacturer or agents of manufacturer holding the Letter of Authority of the

Principal specifically authorizing the agent to make an offer in India in response to EOI/RFP either directly or through the agents/representatives.

2.2.2 The amount of commission /remuneration included in the price(s) quoted by the EOI/RFPer for himself.

2.2.3 Confirmation of the foreign principals of the Tenderer that the commission/ remuneration, if any, reserved for the Tenderer in the quoted price(s), may be paid by RAILTEL in India in equivalent Indian Rupees on satisfactory completion of the Project or supplies of Stores and Spares in case of operation items.

2.3 In either case, in the event of contract materializing, the terms of payment will provide for payment of the commission/ remuneration, if any payable to the agents/representatives in India in Indian Rupees on expiry of 90 days after the discharge of the obligations under the contract.

2.4 Failure to furnish correct and detailed information as called for in paragraph 2.0 above will render the concerned EOI/RFP liable to rejection or in the event of a contract materializing, the same liable to termination by RAILTEL. Besides this there would be a penalty of banning business dealings with RAILTEL or damage or payment of a named sum.

* * * * *

Annexure-B

GUIDELINES ON BANNING OF BUSINESS DEALINGS

1. Introduction

1.1 RailTel Corporation of India Ltd (RAILTEL), being a Public Sector Enterprise, under the administrative control of the Ministry of Railways and therefore being an authority deemed to be 'the state' within the meaning of Article 12 of Constitution of India, has to ensure preservation of rights enshrined in Chapter III of the Constitution. RAILTEL has also to safeguard its commercial interests. RAILTEL deals with Agencies, who have a very high degree of integrity, commitments and sincerity towards the work undertaken. It is not in the interest of RAILTEL to deal with Agencies who commit deception, fraud or other misconduct in the execution of contracts awarded / orders issued to them. In order to ensure compliance with the constitutional mandate, it is incumbent on RAILTEL to observe principles of natural justice before banning the business dealings with any Agency.

1.2 Since banning of business dealings involves civil consequences for an Agency concerned, it is incumbent that adequate opportunity of hearing is provided and the explanation, if EOI/RFPed, is considered before passing any order in this regard keeping in view the facts and circumstances of the case.

2. Scope

2.1 The General Conditions of Contract (GCC) of RAILTEL generally provide that RAILTEL reserves its rights to remove from list of approved suppliers/ contractors or to ban business dealings if any Agency has been found to have committed misconduct and also to suspend business dealings pending investigation. If such provision does not exist in any GCC, the same may be incorporated.

2.2 Similarly, in case of sale of material there is a clause to deal with the Agencies/ customers/ buyers, who indulge in lifting of material in unauthorized manner. If such a stipulation does not exist in any Sale Order, the same may be incorporated.

2.3 However, absence of such a clause does not in any way restrict the right of Company (RAILTEL) to take action / decision under these guidelines in appropriate cases.

2.4 The procedure of (i) Removal of Agency from the List of approved suppliers/ contractors; (ii) Suspension and (iii) Banning of Business Dealing with Agencies, has been laid down in these guidelines.

2.5 These guidelines apply to Corporate Office, all Regions and Subsidiaries of RAILTEL.

2.6 It is clarified that these guidelines do not deal with the decision of the Management to avoid entertaining any particular Agency due to its poor / inadequate performance or for any other reason.

2.7 The banning shall be with prospective effect, i.e., future business dealings.

3. Definitions

In these Guidelines, unless the context otherwise requires:

i) 'Party / Contractor / Supplier / Purchaser / Customer' shall mean and include a public limited company or a private limited company, a firm whether registered or not, an individual, a cooperative society or an association or a group of persons engaged in any commerce, trade, industry, etc. 'Party / Contractor / Supplier / Purchaser / Customer' in the context of these guidelines is indicated as 'Agency'.

ii) 'Inter-connected Agency' shall mean two or more companies having any of the following features:

a) If one is a subsidiary of the other;

b) If the Director(s), Partner(s), Manager(s) or Representative(s) are common;

c) If management is common;

d) If one owns or controls the other in any manner;

iii) 'Competent Authority' and 'Appellate Authority' shall mean the following:

a) For Company (entire RAILTEL) wide Banning: The Director shall be the 'Competent Authority' for the purpose of these guidelines. CMD, RAILTEL shall be the 'Appellate Authority' in respect of such cases except banning of business dealings with Foreign Suppliers of imported items.

b) For banning of business dealings with Foreign Suppliers of imported items, RAILTEL Directors Committee (RDC) shall be the 'Competent Authority'. The Appeal against the Order passed by RDC, shall lie with CMD, as First Appellate Authority.

c) In case the foreign supplier is not satisfied by the decision of the First Appellate Authority, it may approach Railway Board as Second Appellate Authority.

d) For RailTel Regions only: Any officer not below the rank of General Manager appointed or nominated by the Executive Director of concerned Region shall be the 'Competent Authority' for the purpose of these guidelines. The Executive Director of the concerned Region shall be the 'Appellate Authority' in all such cases.

e) For Corporate Office only: For procurement of items / award of contracts, to meet the requirement of Corporate Office only, Concerned Group General Manager / General Manager shall be the 'Competent Authority' and concerned Director shall be the 'Appellate Authority'.

f) CMD, RAILTEL shall have overall power to take suo-moto action on any information available or received by him and pass such order(s) as he may think appropriate, including modifying the order(s) passed by any authority under these guidelines.

iv) 'Investigating Department' shall mean any Department or Unit investigating into the conduct of the Agency and shall include the Vigilance Department, Central Bureau of Investigation, the State Police or any other department set up by the Central or State Government having powers to investigate.

v) 'List of approved Agencies - Parties / Contractors / Suppliers/ Purchaser/ Customers' shall mean and include list of approved /registered Agencies - Parties/ Contractors / Suppliers / Purchasers / Customers, etc.

4. Initiation of Banning / Suspension

Action for banning / suspension of business dealings with any Agency should be initiated by the department having business dealings with them after noticing the irregularities or misconduct on their part. Besides the concerned department, Vigilance Department of each Region / Unit/ Corporate Office may also be competent to initiate such action.

5. Suspension of Business Dealings

5.1 If the conduct of any Agency dealing with RAILTEL is under investigation by any department (except Foreign Suppliers of imported items), the Competent Authority may consider whether the allegations under investigation are of a serious nature and whether pending investigation, it would be advisable to continue business dealing with the Agency. If the Competent Authority, after consideration of the matter including the recommendation of the Investigating Department, if any, decides that it would not be in the interest to continue business dealings pending investigation, it may suspend business dealings with the Agency. The order to this effect may indicate a brief of the charges under investigation. If it is decided that inter-connected Agencies would also come within the ambit of the order of suspension, the same should be specifically stated in the order. The order of suspension would operate for a period not more than six months and may be communicated to the Agency as also to Investigating Department. The

Investigating Department may ensure that their investigation is completed and whole process of final order is over within such period.

5.2 The order of suspension shall be communicated to all the departmental heads within the unit/ region/ Corporate Office as the case may be. During the period of suspension, no business dealing may be held with the agency.

5.3 As far as possible, the existing contract(s) with the Agency may continue unless the Competent Authority, having regard to the circumstances of the case, decides otherwise.

5.4 If the gravity of the misconduct under investigation is very serious and it would not be in the interest of RAILTEL, as a whole, to deal with such an Agency pending investigation, the Competent Authority may send his recommendation to Chief Vigilance Officer (CVO), RAILTEL Corporate Office alongwith the material available. If Corporate Office considers that depending upon the gravity of the misconduct, it would not be desirable for all the units/ regions of RAILTEL to have any dealings with the Agency concerned, an order suspending business dealings may be issued to all the units/ Regions / Corporate Office by the Competent Authority of the Corporate Office, copy of which may be endorsed to the Agency and all concerned. Such an order would operate for a period of six months from the date of issue.

5.5 for suspension of business dealings with Foreign Suppliers of imported items, following shall be the procedure:

i) Suspension of the foreign suppliers shall apply throughout the Company/ Regions including Subsidiaries.

ii) Based on the complaint forwarded by ED / GGM / GM or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of RAILTEL to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director / GGM / GM, to place it before a Committee consisting of the following:

1. ED / GGM/ GM (viz. Representative of Corporate Finance).
2. ED / GGM/ GM (viz. Representative of Department concerned with procurement of imported items)- Convener of the Committee.
3. ED / GGM/ GM (to be nominated on case-to-case basis).

4. ED / GGM/ GM ((viz. Representative of Corporate Law).

The committee shall expeditiously examine the report and give its comments / recommendations within twenty-one days of receipt of the reference by ED/ GGM/ GM.

iii) The comments / recommendations of the Committee shall then be placed by ED/GGM/GM, before RAILTEL Directors' Committee (RDC) constituted for import of items. If RDC opines that it is a fit case for suspension, RDC may pass necessary orders which shall be communicated to the foreign supplier by the ED/GGM/GM.

5.6 If the Agency concerned asks for detailed reasons of suspension, the Agency may be informed that its conduct is under investigation. It is not necessary to enter into correspondence or argument with the Agency at this stage.

5.7 It is not necessary to give any show-cause notice or personal hearing to the Agency before issuing the order of suspension. However, if investigations are not complete in six months' time, the Competent Authority may extend the period of suspension by another three months, during which period the investigations must be completed.

6. Ground on which Banning of Business Dealings can be initiated

6.1 If the security consideration, including questions of loyalty of the Agency to the State, so warrants;

6.2 If the Director / Owner of the Agency, proprietor or partner of the firm, is convicted by a Court of Law for offences involving moral turpitude in relation to its business dealings with the Government or any other public sector enterprises or RAILTEL, during the last five years;

6.3 If there is strong justification for believing that the Directors, Proprietors, Partners, owner of the Agency have been guilty of malpractices such as bribery, corruption, fraud, substitution of EOI/RFPs, interpolations, etc;

6.4 If the Agency continuously refuses to return / refund the dues of RAILTEL without showing adequate reason and this is not due to any reasonable dispute which would attract proceedings in arbitration or Court of Law;

6.5 If the Agency employs a public servant dismissed / removed or employs a person convicted for an offence involving corruption or abetment of such offence;

6.6 If business dealings with the Agency have been banned by the Govt. or any other public sector enterprise;

6.7 If the Agency has resorted to Corrupt, fraudulent practices including misrepresentation of facts;

6.8 If the Agency uses intimidation/ threatening or brings undue outside pressure on the Company (RAILTEL) or its official in acceptance/ performances of the job under the contract;

6.9 If the Agency indulges in repeated and / or deliberate use of delay tactics in complying with contractual stipulations;

6.10 Wilful indulgence by the Agency in supplying sub-standard material irrespective of whether pre-dispatch inspection was carried out by Company (RAILTEL) or not;

6.11 Based on the findings of title investigation report of CBI / Police against the Agency for malafide / unlawful acts or improper conduct on his part in matters relating to the Company (RAILTEL) or even otherwise;

6.12 Established litigant nature of the Agency to derive undue benefit;

6.13 Continued poor performance of the Agency in several contracts;

6.14 If the Agency misuses the premises or facilities of the Company (RAILTEL), forcefully occupies tampers or damages the Company's properties including land, water resources, etc.

(Note: The examples given above are only illustrative and not exhaustive. The Competent Authority may decide to ban business dealing for any good and sufficient reason).

7. Banning of Business Dealings

7.1 Normally, a decision to ban business dealings with any Agency should apply throughout the Company including subsidiaries. However, the Competent Authority of the Region/ Unit

except Corporate Office can impose such ban Region-wise only if in the particular case banning of business dealings by respective Region/ Unit will serve the purpose and achieve its objective and banning throughout the Company is not required in view of the local conditions and impact of the misconduct/ default to beyond the Region/ Unit. Any ban imposed by Corporate Office shall be applicable across all Regions/ Units of the Company including Subsidiaries.

7.2 For Company-wide banning, the proposal should be sent by ED of the Region/ Unit to the CVO/RailTel setting out the facts of the case and the justification of the action proposed alongwith all the relevant papers and documents except for banging of business dealings with Foreign Suppliers of imported items.

The Corporate Vigilance shall process the proposal of the concerned Region/ Unit for a prima-facie view in the matter by the Competent Authority nominated for Company-wide banning.

The CVO shall get feedback about that agency from all other Regions/ Units. Based on this feedback, a prima-facie decision for banning / or otherwise shall be taken by the Competent Authority.

If the prima-facie decision for Company-wide banning has been taken, the Corporate Vigilance shall issue a show-cause notice to the agency conveying why it should not be banned throughout RAILTEL.

After considering the reply of the Agency and other circumstances and facts of the case, a final decision for Company-wide banning shall be taken by the competent Authority.

7.3 There will be a Standing Committee in each Region/ Unit to be appointed by Chief Executive Officer for processing the cases of "Banning of Business Dealings" except for banning of business dealings with foreign suppliers. However, for procurement of items/ award of contracts, to meet the requirement of Corporate Office only, the committee shall be consisting of General Manager/ Dy. General Manager each from Operations, Finance, Law & Project. Member from Project shall be the convener of the committee. The functions of the committee shall, inter-alia include:

i) To study the report of the investigating Agency and decide if a prima-facie case for Company-wide / Region wise banning exists, if not, send back the case to the Competent Authority.
ii) To recommend for issue of show-cause notice to the Agency by the concerned department.

iii) To examine the reply to show-cause notice and call the Agency for personal hearing, if required.

iv) To submit final recommendation to the Competent Authority for banning or otherwise.

7.4 If the Competent Authority is prima-facie of view that action for banning business dealings with the Agency is called for, a show- cause notice may be issued to the Agency and an enquiry held accordingly.

7.5 Procedure for Banning of Business Dealings with Foreign Suppliers of imported items.

i) Banning of the agencies, shall apply throughout the Company including subsidiaries.

ii) Based on the complaint forwarded by Executive Director or received directly by Corporate Vigilance, an investigation shall be carried out by Corporate Vigilance. After investigation, depending upon the gravity of the misconduct, Corporate Vigilance may send their report to Executive Director/ GGM/ GM, to be placed before a Committee consisting of the following:

1. ED / GGM/ GM (viz. Representative of Corporate Finance).
2. ED / GGM/ GM (viz. Representative of Department concerned with procurement of imported items)- Convener of the Committee.
3. ED / GGM/ GM (to be nominated on case to case basis).
4. ED / GGM/ GM ((viz. Representative of Corporate Law).

The Committee shall examine the report and give its comments/ recommendations within 21 days of receipt of the reference by ED.

iii) The comments/recommendations of the Committee shall be placed by ED/ GGM/ GM before RAILTEL Directors' Committee (RDC) constituted for import of foreign items. If RDC opines that it is a fit case for initiating banning action, it will direct

ED/ GGM/ GM to issue show-cause notice to the agency for replying within a reasonable period.

iv) On receipt of the reply or on expiry of the stipulated period, the case shall be submitted by ED to RDC for consideration & decision.

v) The decision of the RDC shall be communicated to the agency by ED/GGM/GM concerned.

8. Removal from List of Approved Agencies – Suppliers/Contractors, etc.

8.1 If the Competent Authority decides that the charge against the Agency is of a minor nature, it may issue a show-cause notice as to why the name of the Agency should not be removed from the list of approved Agencies - Suppliers / Contractors, etc.

8.2 The effect of such an order would be that the Agency would not be disqualified from competing in Open Tender Enquiries but LTE (Limited Tender Enquiry) may not be given to the Agency concerned.

8.3 Past performance of the Agency may be taken into account while processing for approval of the Competent Authority for awarding the contract.

9. Show-Cause Notice

9.1 In case where the Competent Authority decides that action against an Agency is called for, a show-cause notice has to be issued to the Agency. Statement containing the imputation of misconduct or misbehaviour may be appended to the show-cause notice and the Agency should be asked to submit within 15 days a written statement in its defence.

9.2 If the Agency requests for inspection of any relevant document in possession of RAILTEL, necessary facility for inspection of documents may he provided.

9.3 The Competent Authority may consider and pass all appropriate speaking order:

a) For exonerating the Agency if the charges are not established.
b) For removing the Agency from the list of approved Suppliers/ Contactors, etc.
c) For banning the business dealing with the Agency.

9.4 If it decides to ban business dealings, the period for which the ban would be operative may be mentioned. The order may also mention that the ban would extend to the interconnected Agencies of the Agency.

10. Appeal against the Decision of the Competent Authority

10.1 The agency may file an appeal against the order of the Competent Authority banning

business dealing, etc. The appeal shall lie to Appellate Authority. Such an appeal shall be preferred within one month from the date of receipt of the order banning business dealing, etc.

10.2 Appellate Authority would consider the appeal and pass appropriate order which shall be communicated to the Agency as well as the Competent Authority.

11. Review of the Decision by the Competent Authority

Any petition / application filed by the Agency concerning the review of the banning order passed originally by Chief Executive / Competent Authority under the existing guidelines either before or after filing of appeal before the Appellate Authority or after disposal of appeal by the Appellate Authority, the review petition can be decided by the Chief Executive / Competent Authority upon disclosure of new facts / circumstances or subsequent development necessitating such review. The Competent Authority may refer the same petition to the Standing Committee for examination and recommendation.

12. Circulation of the names of Agencies with whom Business Dealings have been banned

12.1 Depending upon the gravity of misconduct established, the Competent Authority of the Corporate Office may circulate the names of Agency with whom business dealings have been banned, to the Government Departments, other Public Sector Enterprises, etc. for such action as they deem appropriate.

12.2 If Government Departments or a Public Sector Enterprise requests for more information about the Agency with whom business dealings have been banned, a copy of the report of the Inquiring authority together with a copy of the order of the Competent Authority / Appellate Authority may be supplied.

12.3 If business dealings with any Agency have been banned by the Central or State Government or any other Public Sector Enterprise, RAILTEL may, without any further enquiry or investigation, issue an order banning business dealing with the Agency and its interconnected Agencies.

12.4 Based on the above, Regions / Units may formulate their own procedure for implementation of the guidelines.

Annexure - C

SCOPE OF WORK

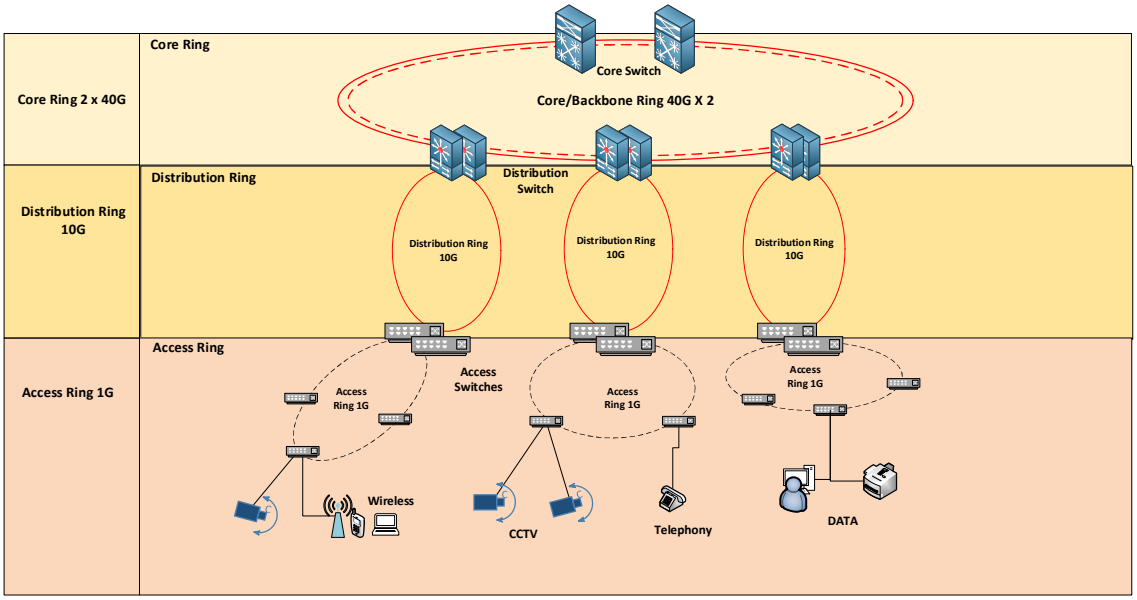
Scope of work for Supply, Installation, testing and commissioning of the project for Education University

The EDUCATION UNIVERSITY campus has multiple academic, admin and residential buildings. This document contains deployment of applications and its backend complete network and compute infrastructure for complete campus including academic, admin and residential buildings.

The initial 10 buildings for Phase – 1 are ***Life Science, Earth Science, Faculty and Staff F2, Faculty and Staff F3, Faculty and Staff F4, Club and Guest House, Utility building, Admin Building, Faculty of Law and Humanity, Faculty of Physics, Chemistry and Maths***
The Following Technologies/Solutions needs to be deployed in the campus -

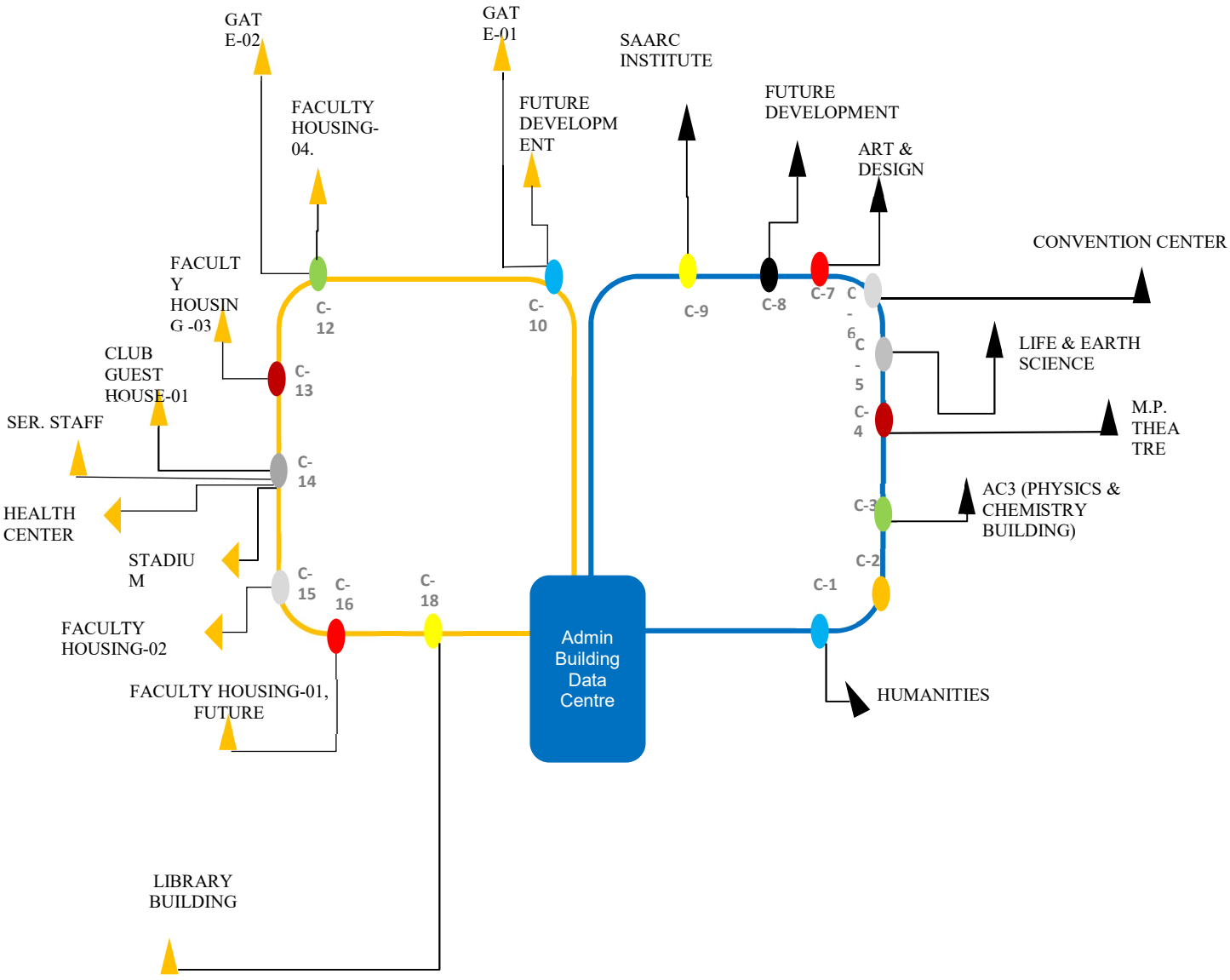
- **Network Setup**
  - The scope covers the network setup for the complete campus which includes 10 buildings with 12000 nodes in phase-1. The main components for the network backbone setup are mentioned below
  - Core switches in Data Centre
  - Distribution switches – Building/block wise and for Perimeter connectivity
  - Access Switches for edge devices
  - Wireless connectivity inside the buildings/Hostels and outdoor hotspots
  - Fiber connectivity is proposed between Data Centre and Building Server/Network Rooms. Centralized Fibre backbone is 144 cores in ring topology. 144 core Fibre cable 2Rings in the existing campus, each ring we have connect 12 distribution points/Buildings.
  - Core to Distribution network connectivity through OS2 Single mode 12/144 core Fibre Cable.
  - Distribution to Access Network connectivity through OS2 Single mode 06 Core Fibre Cable with primary & redundancy. Core to Distribution network with 10G/40G/100G and access with 1G/10G.
  - SITC of passive to be done for 13 Buildings including campus perimeter cabling and passive material required to connect all the nodes mentioned above.

1.1.1. Campus Connectivity (CCTV, WIFI)



- PoE switches are considered for IP phones and Wi-Fi access points connectivity as Power over ethernet is required to run these devices.
- Non-PoE access switches are considered for the data and access control system connectivity as these devices don't required power over the data port.
- Wireless device (Mobile, Laptop) will be connected through the access point to access the network.
- CCTV Cameras will connect on PoE switches and video feeds will be travel through the network and store at the storage for the future usage.
- Data connectivity (Workstation, Printer etc.) will be on 1G copper non-PoE based.
- The uplink from access switches will be connected at distribution switches, two nos of distribution switches are considered for each building.
- Distribution switches will be connected to the core switches placed at the data center with redundant connectivity

Fiber Backbone Logical connectivity Layout:



- **Wireless Connectivity as a part of network set-up**

  - Due to the high density of APs to cover the building and base facilities, centralized controller-based management will use instead of a standalone approach.
  - The solution will allow multiple options to authenticate users with WPA2-PSK, captive portals (open authentication), 802.1x, or WPA2 enterprise, at least.
  - The authentication will perform using internal or external sources, mainly LDAP-based.
  - The solution will allow for multiple networks or SSIDs, associated with different virtual local area networks (VLANs) for differentiated levels of access, including guest, employee and students.
  - WLC solution will provide central management for all the APs in the network, including wireless settings such as channels, power, interference threshold, user authentication
  - The wireless controller will be placed in HA mode in data center.
  - The deployment of both Outdoor and Indoor Access points will be in following way to achieve complete campus network connectivity:
  - The chosen AP models will suffice the physical location of installation, which can be indoor office areas, indoor campus areas, outdoor semi-enclosed areas, or outdoor areas.
  - Indoor APs will install inside the buildings and lobby areas.
  - Outdoor APs will be installed in the outside area of buildings and open area where odd environment conditions are there.
  - There Will Mesh network of Wi-Fi so user can seamlessly roam inside the wireless network.
  - The physical location of AP installation will determine based on the area coverage and number of APs nearby.

Note: For wi-fi Products- Bidder can opt of any of the below option –

Option – 1: UPGRADE: Two Nos of wi-fi controllers & 115 Nos. of access points of existing OEM (M/s Ruckus) to be upgraded for the requirement of the current RFP. Bidder can consider the warranty support cost of existing compatible / usable items and additional cost of new Access Points needed i.e 868 – usable APs.

Option – 2: NEW: Bidder can quote another make for the complete Wi-Fi requirement with buyback of existing setup. Bidder will separately indicate the buyback cost of Two Nos of wi-fi controllers & 115 Nos. of access points while quoting the Wi-Fi solution.

- ## Network Security –
  - Web-Security needs to be deployed in the data centre with the followings components –
    - WAF with 5gbps of throughput
    - NAC for 5000 network devices
    - Single Sign-on for 8000 Users
    - Existing firewall will be utilized for the system setup, the WAF,NAC and SSO needs to be integrated with the existing firewall

- ## CCTV Surveillance
  - This project involves the convergence of multiple type of fields & indoor camera feeds to a common centralized point which is the Data Centre. These cameras will be installed to set-up the complete surveillance inside the campus and along the perimeter wall.
  - There will be Bullet cameras, Dome cameras for indoor surveillance inside the buildings

- For perimeter surveillance along the perimeter wall of the campus Bullet and PTZ cameras will be deployed to monitor the intrusion detection on the perimeter of the campus

For CCTV surveillance requirement is for 5 type of cameras –

- Fixed Dome cameras for Indoor surveillance of buildings
- Fixed Bullet Camera with 150m IR range for Perimeter boundary monitoring
- PTZ Camera for tracking of intrusions/ Incidents monitoring
- Box Cameras for ANPR on Gates for tracking of Number plates
- Fixed UHD camera for Facial recognition system on gates

The details of the cameras which needs to be deployed for surveillance are mentioned below -

Fixed bullet IR Cameras

- The fixed cameras with 150m IR range shall be placed to cover the entire perimeter surveillance area without gap. These are day/night cameras i.e. visible spectrum cameras. By using IR illuminator, they allow imaging of dark scene (Night Mode) thereby providing intelligible image even during dark hours. In the illustration below, a 5km long perimeter security solution is to be provided. The gap between two cameras is planned to be 50m for a gap-free coverage as per the site conditions.

Fixed Dome IR Cameras

- The fixed dome cameras with 50m IR range shall be placed to cover the maximum indoor surveillance area without gap. These are day/night cameras i.e. visible spectrum cameras. By using IR illuminator, they allow imaging of dark scene (Night Mode) thereby providing intelligible image even during dark hours. These cameras will be installed inside the buildings to cover the areas like Classrooms, seminar halls, Lecture theatre, Corridor, entry/exit of buildings and Reception areas

Fixed Box IR Cameras

- The fixed box cameras with 50m IR range shall be placed on the gates to run the application of ANPR. Via these cameras we will be able to capture the number plates of all the vehicles entering and exiting from the campus.

Fixed UHD IR Cameras

- The fixed UHD cameras with 50m IR range shall be placed on the strategic locations with FRS Software. Via these cameras we will be able to capture the picture of students, visitors & Staff. This will help us in locating the blacklisted person if any enters the campus

Pan-Tilt Zoom Cameras

- These have narrower field of view and hence are capable of higher resolution. These camera systems are equipped with motorized pan-tilt capability to be able to cover wider areas while simultaneously a narrower field of view, allows detection at further distances. The Proposed PTZ Camera will acquire 360-degree visuals of the surrounding in darkness, fog, etc. on 24 x 7 basis.

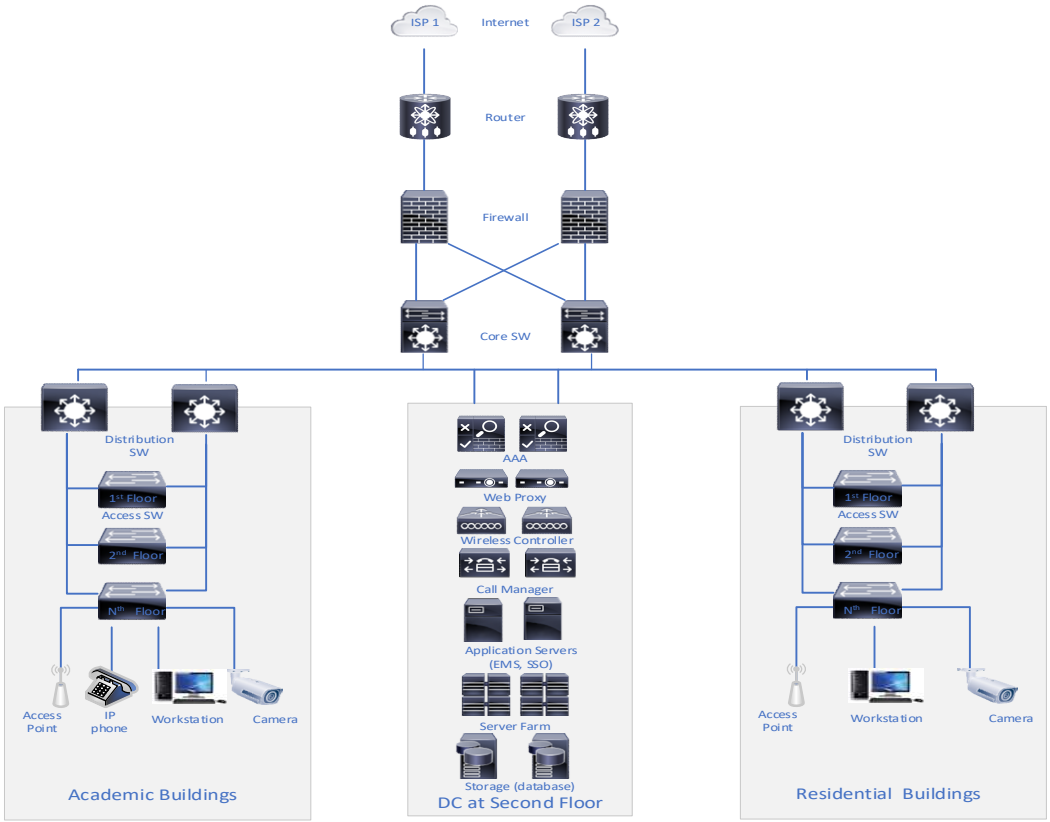
Building wise Cameras to be deployed in Phase-1 are mentioned in the table below -

Phase-1						
Type of Building	**Total**	**FRS**	**Dome**	**PTZ**	**Fixed Box**	**Bullet**
LS	237	1	236	0	0	0
ES	167	1	166	0	0	0
F2	44	0	40	4	0	0

F3	44	0	40	4	0	0
F4	44	0	40	4	0	0
Club and Guest House	51	0	51	0	0	0
Admin	151	2	149	0	0	0
AC3	297	0	297	0	0	0
AC4	238	0	238	0	0	0
Utility	40	0	40	0	0	0
Main Entry Exit & DC	32	6	10	4	6	6
Pheriphery	135	0	0	25	0	110
Total	1480	10	1307	41	6	116

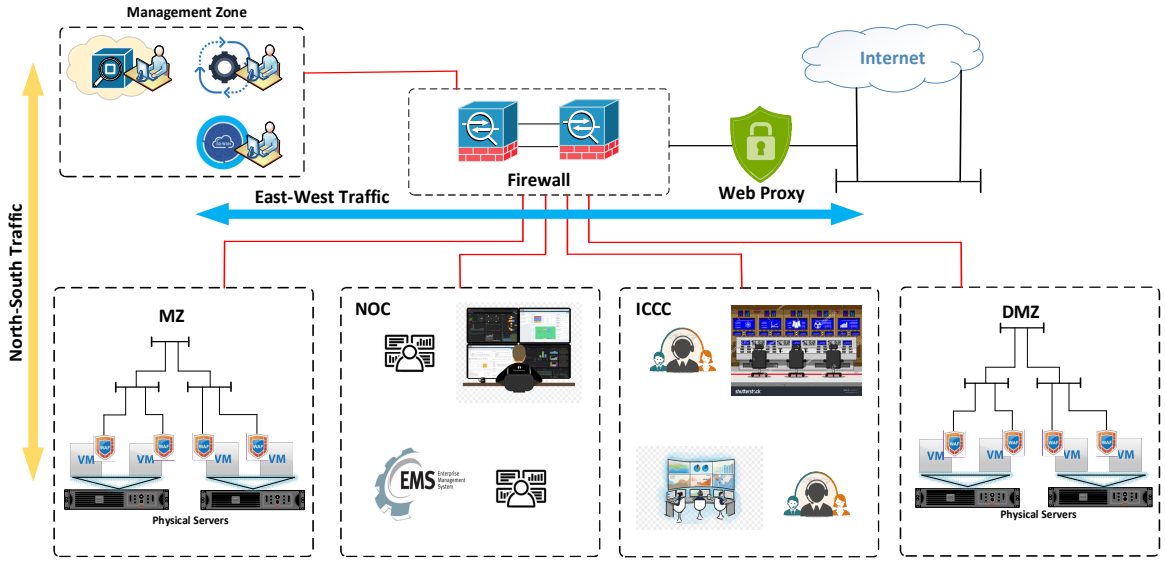
- **Data Centre** –
    - The DC will be located at admin building with capacity of 24 Racks initially (18 New racks and 6 existing) scalable to 30 racks. The compute for applications and core network/security components will be hosted in the data centre
    - At the Data Centre, Tier III provisions will be ensured with High Availability measures for IT and Non- IT associated components. The DC will be prepared with highly secured environment which will enable all Video Management algorithms facilitating and bridging all Video Analytics, Facial Recognition, ANPR, Gate Management outcomes to communicate with Command & Control centre.
    - Non-IT like PAC, False Ceiling, False flooring with electrical components will be provided by EDUCATION UNIVERSITY. Some of the components like Rodent repellent, vesda & Water leak detection system needs to be provided by the System Integrator.
    - UPS also needs to be provided by System Integrator as per the load required of the components proposed by the system integrator.
    - Staging area to be set-up by system integrator with at least sitting area for 10 engineers.
    - Warehouse will be provided by EDUCATION UNIVERSITY at datacenter building.

Architecture for data center is given below -



- Two ISP links will be there for providing internet connectivity to the campus, this links will be from two different ISP for ensure redundancy.
- Both ISP links will be terminated at the Router end, this router will perform routing for the DC network.
- UTM firewall will be act as security gateway for the complete network connecting outside internet to the campus network.
- Security policies will be performed at firewall end which contain UTM license capable for IPS, URL filtering and Anti Malware.
- Two core switches will be deployed in the HA as the backbone of network, firewall will be connected to this core switches and complete DC traffic will be handled by these core switches.
- For building connectivity access and distribution switches are purposed. Various number of access switches will be placed on each floor of both building based on the endpoint's requirement.
- In the data center centralized wireless controller will be placed to manage and configure all the access points are there.
- EMS/NMS will be configured to monitor all the devices in complete network infra
- Workstation and other endpoint devise will be connected through the wire connectivity.
- Server will be used to host various applications and software solution.
- Server Management tool: OEM Server Management Solutions should be in place to support firmware upgrades and fault remediation.

Logical architecture for the EDUCATION UNIVERSITY data center:



- Multiple zones will create on the firewall to breakout the network for security and easy management purpose.
- DMZ zone will be created to host public facing applications in the EDUCATION UNIVERSITY network, this will ensure additional layer of security to the network by segregating the attack surface.
- MZ zone will use to host internal application and other services like NTP, DNS server and database etc.
- Separate management zone will be created to provide the management connectivity to the complete network, by using separate management network we will be able to take management access of devices in case of data connectivity down.
- EMS will be placed in NOC zone for helpdesk and monitoring for infrastructure monitoring like network, security, server etc.
- A separate ICCC zone will use to host ICCC applications and CCTV monitoring.
- Communication between various zones will be on requirement and demand basis as per the EDUCATION UNIVERSITY network.

• Storage for complete set-up

- Data centre storage is the collective term used to define the tools, technologies, and processes to design, implement, manage, and monitor storage infrastructure and resources within a data centre. It is part of the data centre infrastructure and includes all IT/data centre assets that directly or indirectly play a part in storage within a data center.
- Minimum required for the storage is 2.5 PB as per the calculation for storing application data, video feeds and other solution, However if System Integrator needs more storage as per there solution than SI needs to provide extra storage without any cost implication
- Data centre storage primarily refers to the devices, equipment and software technologies that enable data and application storage within a data center facility.
- Storage includes Hard disk drives, tape drives and other forms of internal and external storage
- Storage and backup management software utilities
- External storage facilities/solutions such as cloud or remote storage
- It also includes data center storage policy and procedures that govern the entire process of data storage and retrieval. Moreover, data center storage may also incorporate data center storage security and access control procedures and methodologies.
- Additional SAN switches in HA mode to be provided with the solution as per the bidder solution.

- **Integrated Command & Control Centre –**

  - Centralized command & Control center needs to be setup at EDUCATION UNIVERSITY which will be located at the admin building and will be having the 12 operator workstations.
  - The scope of ICCC is limited to integration, definition of standard operating procedures, incident management, resource management for scoped subsystems. ICCC shall provide standard interfaces for third party components for future extensions.
  - ICCC aggregates all the information from sub-components. The alerts which are automatically generated by smart field elements are routed through the standard operating procedures, which can be defined as per campus needs.
  - There will be deployment of Video Management system will act as a central bridging point in between the Command & Control, Visualization layer (Video-wall and display screens) and the storage at DC. Recording of all the cameras will be stored in Storage hosted in data centre for 30 days.

- **Video Management system**

  - Video Management Software (VMS) plays a vital role in today's security and surveillance scenario. Data captured and stored through VMS are analysed for forensic purposes. Situational analytics are implemented over the VMS for more efficient and directional data capture.
  - A video Management system with 2500 licenses to be provided and installed in the data centre which will have approx. 1500 cameras for phase-1 and additional 1000 cameras for phase-2
  - Servers for VMS to be provided in N+1 Configuration for failover. Minimum Specifications for the VMS servers is provided, if higher sizing will be required then system integrator need to quote as per there requirement.
  - VMS software needs to be integrated with ICCC, FRS, VA & Gate Management system
  - Viewing of the live Camera Video Streams (Approx. 10% of 1000 Camera) based on access rights
  - Viewing rights to the stored feeds, stored on Primary / Secondary Storage
  - Viewing of video feeds from collaborative public CCTV surveillance system
  - Viewing of video feeds basis upon the Alerts / Exceptions / Triggers raised by Video Analytics, FRS and ANPR Solution.
  - Trail Report on specific person / object / vehicle for a specific period / location
  - Personalized Dashboard (depending upon role-based access level defined to the police personnel/ operators, detailed requirement finalization will be done during Pre-Implementation stage).
  - Provide search of recorded video. Advanced search should be possible based on various filters like alarm / event, area, camera, etc.
  - Export rights of video / other critical incident data based on appropriate rights and privileges.

- **AI based Video Analytics**

  - The Video Analytics using AI and ML methodologies is the driving force behind the success of this project and the useful impacts of all the investments done in the envisaged project. The System Integrator is subjected to write and execute well considered SoPs and workflows of all the use-cases as desired to make this project a success. The implemented platform will be used to leverage video feeds from existing/ planned cameras in other schemes as well.

  - Video Analytics will run on all the perimeter cameras and 20% of other cameras.

- Type of analytics required are mentioned below –
  - Intrusion detection on the perimeter wall
  - People count for outdoor cameras
  - Loitering
  - Crowd Detection
  - People fight detection
  - Abandoned object

- **Facial Recognition System**

  - Facial Recognition application to be deployed on 3 entry and exit points and other strategic locations of the EDUCATION UNIVERSITY building.

  - Face Recognition System shall work on real time and offline mode for identifying or verifying a person from various kinds of inputs from digital image file and live video source from any IP video streaming sensor like IP Camera, Body Worn Cameras, Mobile handset cameras, UAV/Drones etc. We are proposing 10 Nos FRS cameras in phase 1 SOR A and 3 Nos FRS cameras in Phase 2.

  - Server sizing for FRS applications to be provided by System Integrator as per there solution, However minimum specifications for FRS server is mentioned in the technical specs

- **EMS and Helpdesk Management**

  - The EMS/NMS applications needs to be installed in Data Centre for monitoring and managing the network devices.

  - The total licenses required for Ph-1 is 5000 Approx. MSI needs to quote the license accordingly, As all the switches, wi-fi-access points, cameras, servers and applications to be monitored by EMS tool.

  - Basic Features of EMS/NMS Application
    - Auto discovery & Topology
    - Service Monitoring
    - Data Processing
    - Root Cause Analysis
    - Probable Cause Analysis
    - Service Impact Analysis
    - Threshold Crossing Alerts
    - Network Protocol Alarm
    - Event Correlation
    - Alert Notification
    - Dashboards

  - Helpdesk System should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents. It will be responsible for the ticketing handling. Tickets will be automatically created for the NMS. The ITSM solution should be also will manage the assets & hardware inventory.

- **Visitor Management System**

  - Visitor Management system needs to be installed on all the 3 gates of the campus and needs to be integrated with ICCC.

- Complete details of the visitors to be stored in the Data centre for at-least 3 years.

- The followings modules to be the part of the system proposed
  - Admin, Employee / Host and Security Gate module
  - Gate pass creation
  - Bar code / QR Code Integration
  - Ban/pre approve/under watch visitors
  - Multiple gates supported
  - Dynamic Gate-pass design (user can design the Gate-pass) & printing supported
  - Comprehensive reporting
  - Intuitive and simple interface for security user
  - Visitor data capturing –personal information, company information, material carrying, vehicle details, host employee and other details
  - Visitor OTP Authentication
  - Intimate host about visitor by SMS, pop up on PC, email or through the system
  - Visitor Fingerprint Capture (Optional)
  - Barcode / OR Code based Visitor Exit

• Smart Classroom

- These are technology-enhanced classrooms that foster opportunities for teaching and learning by integrating learning technology in the conventional classroom setup. The smart classes help teachers to deliver lectures more effectively for providing a better learning experience to the students. In phase 1- SOR A, there are 85 Nos Classroom where smart classroom has to be deployed.

- Followings will be the part of smart classroom solution.

- Interactive Display based Smart Classroom
  - –75 inch LED Screen that connects with a computing device. The teacher should has option to conduct the class using a Stylus, finger or Wireless Mouse and Keyboard.

  - Facial Recognition based attendance system

• Gate Management System

- For Gate Management followings solutions needs to be deployed in all the 3 entry/exit gates of the campus
  - **ANPR System** – ANPR System with cameras needs to be installed on all entry/exit gates of the campus. System should capture number plates of all the vehicles entering and exiting from the campus. Database of all the vehicles should be stored for 1 year with proper date and time stamping.

  - **X Ray Baggage Scanner** for Security Check-In Baggage Scanners needs to be installed for entry only.

  - **Boom Barrier with RFID -** Boom Barrier is also known as a gate barrier carries a pole that hangs to one endpoint at a vertical boom which is offset by some distance. The boom ascends and descends by making use of a geared motor that ensures gradual procedure and additionally the pole is counter top weighed to support the distribution of weight. Automatic barriers are the first instant of physical security solutions that are used to control vehicle entry and it will be install at Entry/Exit Side of Gate. We will propose 6 Nos. boom barrier system to control unwanted entry of vehicles inside the university premises.

- **RFID –** Boom barrier needs to be integrated with RFID reader. The employees which will have the access to the parking should enter the premised with the help of RFID tags. RFID reader to be integrated with Access control system to provide access to the registered users.

- ## IPBAX System

  - IPBX system needs to be installed in the campus which will support 1000 IP phones for the faculty/admin buildings and 350 Analog phones for Hostel.
  - Single system should be provided which will support both IP and Analog phones
  - Helpdesk Phones to be provided on all the Receptions of the buildings.
  - IP phone should be provisioned for visitor Management room and Analog phones for all the 3 Entry/Exit Gates of Campus. Buildings wise details of IP/Analog Phones will be provided during installation.
  - PRI Line will be provided by EDUCATION UNIVERSITY

Annexure - D

TECHNICAL COMPLIANCE

A.1	Full HD Fixed dome type IP colour camera		
Item. No	Description	Specifications	Compliance
1	Type of Camera	Vandal Dome	
2	Image Sensor	1/2.7" or better progressive Scan CMOS	
3	Signal System	PAL/NTSC	
4	Resolution & frame rate	5MP (2592×1944)@20fps, 4MP (2688 × 1520)@ 25/30fps	
5	Minimum Illumination	0.008Lux@ F1.6, AGC ON, 0 lux with IR or better	
6	Imaging	1/3s to 1/12000s, Auto Gain Control , White Balance- Auto, Back Light Compensation, Multi zone Privacy Masking, HLC.	
7	Signal to Noise Ratio	50 dB or more	
8	Lens Type	4.5mm (±1mm) ~ 10mm (±1mm) or Better	
9	Focus	Motorized Vari Focal	
10	DORI Distance	W– 62.9m T-183m or better	
11	Day & Night	True Day & Night High Performance Mechanical IR cut filter with auto switch, IR Source- Inbuilt Smart IR LED's with effective distance upto 30 Mtr or better with the help of External/ Integrated IR.	
12	Video Compression (Minimum)	H.265, H.264	
13	Wide Dynamic Range	WDR (120db or more), HLC and BLC	
14	Digital Noise Reduction	DNR (2D/3D) On/Off	
15	Streaming	Triple streaming , configurable Main stream : 2592 × 1944@1~20 fps or better, (2688 × 1520@1~25/30 fps) Stream 2 : 704 × 576 @1~25/30 fps Stream 3 : 1280 × 720 @1~25/30 fps	
16	Connectivity	LAN	
17	Image Setting	Rotate Mode, saturation, brightness, contrast, sharpness adjustable through client software or web browser	
18	Profile Management	User configuration import, export	
19	Security	User Authentication, Water Marking	
20	Onboard Storage	Camera should support built in Class-10 Micro SD/SDHC/SDXC Card slot upto 256 GB .	
21	Recording Management	Format SD, overwrite, storage management, video to NAS device, remote archive access via FTP login	

22	Edge based Video Analytics & Alarm Trigger	Motion detection, Scene Change, Audio Detection, Camera Tampering alarm, IP address conflict, Storage full, Storage error, Tripwire, Intrusion.	
	Network Compatibility		
23	Network Protocol	IPv4/v6, HTTP, HTTPS, TCP, UDP, ARP, RTP, RTSP, RTCP, RTMP, SMTP, FTP, SFTP, DHCP, DNS, DDNS, QoS, UPnP, NTP, Multicast, ICMP, IGMP, NFS, PPPoE, SNMP, CGI, P2P.	
24	Cyber Security	Encryption for Video, firmware & configuration, Digest, WSSE, account, lockout, security logs, IP/MAC filtering, generation and importing of X.509 certification, syslog, HTTPS, 802.1x, trusted boot, trusted execution, trusted upgrade.	
25	User Access	5 User Simultaneously or more and Minimum 20 User Account supported.	
26	System Capability	It should support ONVIF (Profile S, Profile G and Profile T). The Quoted Model Should be listed on ONVIF Official website. CCTV Camera OEM should be fulltime member of ONVIF and should not be blaclisted/ suspanded by ONVIF.	
27	Video / Evidence Seaching	Camera shall be capable to work together with Smart NVR to perform refine intelligent search, event extraction and merging to event videos.	
28	Ethernet	1 RJ 45 10/100 Ethernet port	
29	Audio In/ Out	Required	
30	Alarm In/ out	Mini. 1 Input & 1 Output port for external sensors etc.	
31	Power Input	Standard DC Jack	
32	Power Requirement	12VDC ± 10%, PoE (IEEE802.3 af)	
33	Power Consumption	Max 20 W	
34	Enclosure	IP66 weather proof and IK10 Vandal Proof or better.	
35	Operating Condition	-20°C to 55°C, humidity 95% (max) (non-condensing)	
36	Standards	UL, CE, FCC, RoHS, BIS Certified	

A.2	Full HD Bullet type IP colour camera		
Item. No	Description	Specifications	Compliance
1	Type of Camera	Outdoor Bullet/ Box Camera	
2	Image Sensor	1/2.8" or better progressive Scan CMOS	
3	Signal System	PAL/NTSC	
4	Resolution & frame rate	2MP (1920 × 1080) @ 25/30fps	
5	Minimum Illumination	0.005Lux@ F1.5, AGC ON, 0 lux with IR or better	
6	Imaging	1/3s to 1/12000s, Auto Gain Control , White Balance- Auto, Back Light Compensation, Multi zone Privacy Masking, HLC.	
7	Signal to Noise Ratio	50 dB or more	
8	Lens Type	5mm (±2mm) ~ 64mm (±2mm) or Better	

9	Focus	Motorized Vari Focal	
10	Day & Night	True Day & Night High Performance Mechanical IR cut filter with auto switch, IR Source- Inbuilt Smart IR LED's with effective distance upto 90 Mtr or better with the help of External/ Integrated IR.	
11	Video Compression (Minimum)	H.265, H.264	
12	Wide Dynamic Range	WDR (120db or more), HLC and BLC	
13	Digital Noise Reduction	DNR (2D/3D) On/Off.	
14	Streaming	Triple streaming , configurable	
15	Connectivity	LAN	
16	Image Setting	Rotate Mode, saturation, brightness, contrast, sharpness adjustable through client software or web browser. Also it should support Defog, RoI & EIS.	
17	Profile Management	User configuration import, export	
18	Security	User Authentication, Water Marking	
19	Onboard Storage	Camera should support built in Class-10 Micro SD/SDHC/SDXC Card slot upto 256 GB .	
20	Recording Management	Format SD, overwrite, storage management, video to NAS device, remote archive access via FTP login	
21	Edge based Video Analytics & Alarm Trigger	Motion detection, Scene Change, Audio Detection, Camera Tampering alarm, IP address conflict, Storage full, Storage error, Tripwire, Intrusion, Perimeter Protection	
	Network Compatibility		
22	Network Protocol	IPv4/v6, HTTP, HTTPS, TCP, UDP, ARP, RTP, RTSP, RTCP, RTMP, SMTP, FTP, SFTP, DHCP, DNS, DDNS, QoS, UPnP, NTP, Multicast, ICMP, IGMP, NFS, PPPoE, SNMP, CGI, P2P.	
	Cyber Security	Encryption for Video, firmware & configuration, Digest, WSSE, account, lockout, security logs, IP/MAC filtering, generation and importing of X.509 certification, syslog, HTTPS, 802.1x, trusted boot, trusted execution, trusted upgrade.	
23	User Access	5 User Simultaneously or more	
24	System Capability	It should support ONVIF (Profile S, Profile G and Profile T). The Quoted Model Should be listed on ONVIF Official website. The proposed CCTV OEM should not be blaclisted/ suspanded by ONVIF.	
25	VMS	Camera shall support open source VMS	
26	Ethernet	1 RJ 45 10/100 Ethernet port	
27	Audio In/ Out	Mini. 1 Input & 1 Output port for external Mix & Speaker.	
28	Alarm In/ out	Mini. 2 Input & 1 Output port for external sensors etc.	
29	Power Input	Standard DC Jack	
30	Power Requirement	12VDC ± 10%, PoE (IEEE802.3 af), ePoE	
31	Power Consumption	Max 20 W	
32	Enclosure	IP67 weather proof and IK10	

33	Operating Condition	-20°C to 55°C, humidity 95% (max) (non-condensing)	
34	Standards	UL, CE, FCC, RoHS, BIS Certified	

A.3	Full HD P/T/Z type IP colour camera:		
Item. No	Description	Specifications	Compliance
1	4MP IP IR PTZ Camera	Motorized PAN TILT ZOOM with IR	
2	Image Sensor	1/2.8" or better progressive Scan CMOS	
3	Signal System	PAL/NTSC	
4	Resolution & frame rate	2MP @ 25/30fps or better	
5	Minimum Illumination	0.005Lux@ F1.6, AGC ON, 0 lux with IR, or better	
6	Imaging	1/1s to 1/12000s, Auto Gain Control , White Balance- Auto, Back Light Compensation, Multi zone Privacy Masking(upto 24 area), HLC	
7	Signal to Noise Ratio	55 dB or more	
8	Lens Type	Focal Length: varifocal 5mm~150mm or better, Focus Adjustment: Automatic, manual	
9	Zoom	30 x Optical zoom or better	
10	Day & Night	True Day & Night High Performance Mechanical IR cut filter with auto switch, IR Source- Inbuilt Smart IR LED's with effective distance. The camera should have IR LED's and cover distance up to 150 mtr. or above	
11	Auto Tracking	The camera should be equipped with auto tracking function using simultaneously all of the panning, tilting and zooming should be available. When a motion is detected in a registered monitoring area, the camera should track the motion (object) and capture it.	
12	Pre/Post Event Buffering	The camera should support atleast of 5 seconds of pre & post event buffering.	
13	PAN Travel	Pan: 0° ~ 360° endless;Manual Pan: 300° /s, Preset : 400° /s	
14	Tilt Travel	Tilt: -15° ~ 90°, auto flip 180°, Manual Tilt: 200° /s, Preset : 300° /s	
15	Presets	300 Presets	
16	Event Notification	Through Relays, E-Mails or FTP	
17	Video Compression (Minimum)	H.265, H.264	
18	Wide Dynamic Range	WDR (120db or more), HLC & BLC	
19	Digital Noise Reduction	DNR (2D+3D) On/Off	
20	Streaming	Triple Streaming,configuable	
21	Connectivity	LAN	

22	Image Setting	Rotate Mode, ROI ,EIS, Defog, saturation, brightness, contrast, sharpness adjustable through client software or web browser	
23	Profile Management	User configuration import, export	
24	Security	User Authentication, Water Marking-	
25	Onboard Storage	Camera should support built in Class-10 Micro SD/SDHC/SDXC Card slot upto 256 GB .	
26	Recording Management	Format SD, overwrite, storage management, video to NAS device, remote archive access via FTP login	
27	Edge based Video Analytics & Alarm Trigger	Motion detection, Scene Change, Audio Detection, Camera Tampering alarm, IP address conflict, Storage full, Storage error, Tripwire, Intrusion.	
	Network Compatibility		
28	Network Protocol	TCP/IP/ICMP, HTTP, HTTPS, SSL, UDP, UPnP, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, SMTP, SNMP, IGMP, 802.1X, QoS, IPv4/v6, Bonjour.	
29	User Access	5 User Simultaneously or more	
30	System Capability	It should support ONVIF (Profile S, Profile G and Profile T). The Quoted Model Should be listed on ONVIF Official website. The proposed CCTV OEM should not be blaclisted/ suspended by ONVIF.	
31	VMS	Camera shall support open source VMS	
32	Ethernet	1RJ 45 10/100 Ethernet port	
33	Power Input	Standard DC Jack	
34	Power Requirement	24 VDC, 2.5 A (± 25%) PoE+ (802.3at)	
35	Power Consumption	Not to exceed 24W when IR on	
36	Enclosure	IP66 weather proof and IK10 Vandal Proof or better	
37	Operating Condition	-20°C to 55°C, humidity 95% (max) (non-condensing)	
38	Audio Support	Audio Interface : The camera should have 1/1 Audio In/Out to connect External Mic and Speaker Audio Compression : G.711a/ G.711u/ PCM	
39	Alarm In/Out	Alarm In/out- 2/1 Ch In/Out	
40	Standards	UL, CE, FCC, RoHS, BIS Certified	

A.4	Digital Key-Board (Joystick)		
Item. No	Description	Specifications	Compliance
		As per Industry standard to meet the solution requirement	

A.5	4K UHD Bullet type IP colour camera		
Item. No	Description	Specifications	Compliance
1	Type of Camera	IP Bullet Camera	
2	Image Sensor	1/1.8" or better progressive Scan CMOS	
3	Signal System	PAL/NTSC	
4	Resolution & frame rate	8 MP (3840× 2160)@25/30fps	
5	Minimum Illumination	0.008Lux@ F1.4, AGC ON, 0 lux with IR or better	
6	Imaging	1/3s to 1/12000s, Auto Gain Control , White Balance- Auto, Back Light Compensation, Multi zone Privacy Masking, HLC.	
7	Signal to Noise Ratio	50 dB or more	
8	Lens Type	4.5 mm (±1mm) ~ 10 mm (±1mm) or Better	
9	Focus	Motorized Vari Focal	
10	DORI Distance	W– 62.9m T– 183m Or better	
11	Day & Night	True Day & Night High Performance Mechanical IR cut filter with auto switch, IR Source- Inbuilt Smart IR LED's with effective distance upto 30 Mtr or better with the help of External/ Integrated IR.	
12	Video Compression (Minimum)	H.265, H.264	
13	Wide Dynamic Range	WDR (120db or more), HLC and BLC	
14	Digital Noise Reduction	DNR (2D/3D) On/Off	
15	Streaming	Quad streaming , configurable Main stream: 8MP/5MP/4MP/3MP/1080P/1.3M/720P/D1 (1 fps–25/30 fps) Sub stream: 1080P/1.3M/720P/D1 (1 fps–15 fps) Third stream: D1/CIF (1 fps–15 fps) Fourth stream: D1/CIF (1 fps–10 fps)s	
16	Connectivity	LAN	
17	Image Setting	Rotate Mode, saturation, brightness, contrast, sharpness adjustable through client software or web browser	
18	Profile Management	User configuration import, export	
19	Security	User Authentication, Water Marking	
20	Onboard Storage	Camera should support built in Class-10 Micro SD/SDHC/SDXC Card slot upto 256 GB .	
21	Recording Management	Format SD, overwrite, storage management, video to NAS device, remote archive access via FTP login	
22	Edge based Video Analytics & Alarm Trigger	Face Detection, People Counting, loitering detection, Motion detection, Human Detection, Vehicle detection, Scene Change, Audio Detection, Camera Tampering alarm,	

		IP address conflict, Storage full, Storage error, Tripwire, Intrusion.	
	Network Compatibility		
23	Network Protocol	IPv4/v6, HTTP, HTTPS, TCP, UDP, ARP, RTP, RTSP, RTCP, RTMP, SMTP, FTP, SFTP, DHCP, DNS, DDNS, QoS, UPnP, NTP, Multicast, ICMP, IGMP, NFS, PPPoE, SNMP, CGI, P2P.	
24	Cyber Security	Encryption for Video, firmware & configuration, Digest, WSSE, account, lockout, security logs, IP/MAC filtering, generation and importing of X.509 certification, syslog, HTTPS, 802.1x, trusted boot, trusted execution, trusted upgrade.	
25	User Access	5 User Simultaneously or more and Minimum 20 User Account supported.	
26	System Capability	It should support ONVIF (Profile S, Profile G and Profile T). The Quoted Model Should be listed on ONVIF Official website. CCTV Camera OEM should be fulltime member of ONVIF and should not be blaclisted/ suspanded by ONVIF.	
27	Video / Evidence Seaching	Camera shall be capable to work together with Smart NVR to perform refine intelligent search, event extraction and merging to event videos.	
28	Ethernet	1 RJ 45 10/100 Ethernet port	
29	Audio In/ Out	Mini. 1 Input & 1 Output port for external Mix & Speaker.	
30	Alarm In/ out	Mini. 2 Input & 1 Output port for external sensors etc.	
31	Power Input	Standard DC Jack	
32	Power Requirement	DC 12V (±30%), PoE (802.3af), ePoE	
33	Power Consumption	Max 20 W	
34	Enclosure	IP67 weather proof and IK10 Vandal Proof.	
35	Operating Condition	-20°C to 55°C, humidity 95% (max) (non-condensing)	

A.6	Fixed Box IP colour camera		
Item. No	Description	Specifications	Compliance
1	Type of Camera	Outdoor Bullet/ Box Camera	
2	Image Sensor	1/1.8" or better progressive Scan CMOS	
3	Signal System	PAL/NTSC	
4	Resolution & frame rate	2688 × 1520@25fps or better	
5	Imaging	1/3s to 1/12000s, Auto Gain Control , White Balance- Auto, Back Light Compensation, HLC.	
6	Lens Type	8mm (±2mm) ~ 40mm (±2mm) or Better	

7	Focus	Motorized Vari Focal	
8	Day & Night	True Day & Night High Performance Mechanical IR cut filter with auto switch, IR Source- Inbuilt four Smart IR LED's with effective distance upto 30 Mtr or better with the help of External/ Integrated IR.	
9	Video Compression (Minimum)	H.265, H.264	
10	Wide Dynamic Range	WDR (80db or more), HLC and BLC	
11	Digital Noise Reduction	DNR (2D/3D) On/Off.	
12	Streaming	Main Stream : 2688 × 1520@25fps Sub Stream : 1600 × 1200@25fps	
13	Connectivity	LAN	
14	Image Setting	Rotate Mode, saturation, brightness, contrast, sharpness adjustable through client software or web browser.	
15	Profile Management	User configuration import, export	
16	Security	User Authentication, Water Marking	
17	Onboard Storage	Camera should support built in Class-10 Micro SD/SDHC/SDXC Card slot upto 256 GB .	
18	Recording Management	Format SD, overwrite, storage management, video to NAS device, remote archive access via FTP login	
	Network Compatibility		
19	Network Protocol	IPv4/v6, HTTP, HTTPS, TCP, UDP, ARP, RTP, RTSP, RTCP, RTMP, SMTP, FTP, SFTP, DHCP, DNS, DDNS, QoS, UPnP, NTP, Multicast, ICMP, IGMP, NFS, PPPoE, SNMP, CGI, P2P.	
20	User Access	5 User Simultaneously or more	
21	System Capability	It should support ONVIF (Profile S, Profile G and Profile T). The Quoted Model Should be listed on ONVIF Official website. The proposed CCTV OEM should not be blaclisted/ suspanded by ONVIF.	
22	Ethernet & Other Interfaces	1 RJ 45 10/100 Ethernet port, 1x RS-485, 1x RS-232	
23	Audio In/ Out	Mini. 1 Input & 1 Output port for external Mix & Speaker.	
24	Alarm In/ out	Mini. 2 Input & 2 Output port for external sensors etc.	
25	Power Requirement	12VDC ± 10%, PoE	
26	Power Consumption	Max 20 W	
27	Enclosure	IP67 weather proof and IK10	
28	Operating Condition	-20°C to 55°C, humidity 95% (max) (non-condensing)	
29	Standards	UL, CE, FCC, RoHS, BIS Certified	
30	LPU	LPU to be provided as per the solution proposed by SI	

B.1	Server for Video Management system		
S.No	Parameter	Specification	Compliance (Yes/ No)
1	Rack Height	4U or lower	
2	CPU Support	Must support 2 CPU's	
3	Processors	minimum 2 processor with 16 Cores or better	
4	Processor Clock Speed	2.5GHz or better	
5	Memory	Minimum 64GB RAM per server	
6	Hard Drives	Minimum 2 X 600GB SAS drives, 4 X 1TB SAS 7200 RPM	
7	RAID Card	RAID Controller Card supports RAID 1, 5 or better	
8	PCI Slots (I/O)	2xPCIe Slots or better	
9	NIC ports	Minimum 4x1G ports	
10	HBA ports	Minimum 2 X 8/16G FC ports	
11	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12	Out-of-Band	Must Support 1G Out of Band connectivity	
13	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	
14	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
15	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management & system health	
16	Warranty	As per RFP requirement	

B.2	Server Video Recording		
S.No	Paramter	Specification	Compliance (Yes/ No)
1	Rack Height	4U or lower	
2	CPU Support	Must support 2 CPU's	
3	Processors	16 Cores or better	
4	Processor Clock Speed	2.5GHz or better	
5	Memory	Minimum 32GB RAM per server	
6	Hard Drives	Minimum 4 X 600GB SAS drives 7200 RPM	
7	RAID Card	RAID Controller Card supports RAID 1, 5 or better	
8	PCI Slots (I/O)	2xPCIe Slots or better	
9	NIC ports	Minimum 4x1G ports	
10	HBA ports	Minimum 2 X 8/16G FC ports	
11	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12	Out-of-Band	Must Support 1G Out of Band connectivity	
13	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	
14	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	

15	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management & system health	
16	Warranty	As per RFP requirement	

B.3	Server for Video Analytics		
S.No	Parameter	Specification	Compliance (Yes/ No)
1	Rack Height	4U or lower	
2	CPU Support	Must support 2 CPU's	
3	Processors	2 X 24 Cores per processor or more	
4	Processor Clock Speed	2.5GHz or better	
5	Memory	Minimum 128GB RAM per server	
6	Hard Drives	Minimum 4 X 1TB SAS drives	
7	GPU Support	Minimum 2 GPU's with minimum 64GB RAM each or better as per solution requirement	
8	RAID Card	RAID Controller Card supports RAID 1, 5, or better	
9	PCI Slots (I/O)	2 x PCIe Slots or better	
10	NIC ports	Minimum 2x10G ports	
11	HBA ports	Minimum 2 X 8/16G FC ports	
12	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
13	Out of Band Connectivity	Must Support 1G Out of Band connectivity	
14	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	
15	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
16	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, & system health	
17	Warranty	As per RFP requirement	

B.4	**Server for Facial Recognition System**		
S.No	Parameter	Specification	Compliance (Yes/ No)
1	Rack Height	4U or lower	
2	CPU Support	Must support 2 CPU's	
3	Processors	2 X 24 Cores per processor or more	
4	Processor Clock Speed	3.0GHz or better	
5	Memory	Minimum 128GB RAM per server	
6	Hard Drives	Minimum 4 X 1TB SAS drives	
7	GPU Support	Minimum 4 GPU's with minimum 64GB RAM each or better as per solution requirement	
8	RAID Card	RAID Controller Card supports RAID 1, 5, or better	
9	PCI Slots (I/O)	2 x PCIe Slots or better	

10	NIC ports	Minimum 2x10G ports	
11	HBA ports	Minimum 2 X 8/16G FC ports	
12	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
13	Out of Band Connectivity	Must Support 1G Out of Band connectivity	
14	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	
15	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
16	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, & system health	
17	Warranty	As per RFP requirement	

B.5	Server for EMS System		
S.No	Paramter	Specification	Compliance (Yes/ No)
1	Rack Height	4U or lower	
2	CPU Support	Must support 2 CPU's	
3	Processors	24 Cores or better	
4	Processor Clock Speed	2.5GHz or better	
5	Memory	Minimum 64GB RAM per server	
6	Hard Drives	Minimum 2 X 600GB SAS drives	
7	RAID Card	RAID Controller Card supports RAID 1, 5 or better	
8	PCI Slots (I/O)	2xPCIe Slots or better	
9	NIC ports	Minimum 4x1/10G ports	
10	HBA ports	Minimum 2 X 8/16G FC ports	
11	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12	Out-of-Band	Must Support 1G Out of Band connectivity	
13	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	
14	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
15	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management & system health	
16	Warranty	As per RFP requirement	

B.6	Server for ICCC Application		
S.No	Parameter	Specification	Compliance (Yes/ No)
1	Rack Height	4U or lower	
2	CPU Support	Must support 2 CPU's	

3	Processors	2 X 24 Cores per processor or more	
4	Processor Clock Speed	3.0GHz or better	
5	Memory	Minimum 128GB RAM per server	
6	Hard Drives	Minimum 4 X 1TB SAS drives	
7	RAID Card	RAID Controller Card supports RAID 1, 5 or better	
8	PCI Slots (I/O)	2xPCIe Slots or better	
9	NIC ports	Minimum 4x1G ports	
10	HBA ports	Minimum 2 X 8/16G FC ports	
11	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12	Out-of-Band	Must Support 1G Out of Band connectivity	
13	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	
14	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
15	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management & system health	
16	Warranty	As per RFP requirement	

B.7	Server/Workstation for Visitor Management System		
S.No	Parameter	Specification	Compliance (Yes/ No)
1	Rack Height	4U or lower	
2	CPU Support	Must support 2 CPU's	
3	Processors	16 Cores or better	
4	Processor Clock Speed	2.5GHz or better	
5	Memory	Minimum 32GB RAM per server	
6	Hard Drives	Minimum 2 X 600GB SAS drives	
7	RAID Card	RAID Controller Card supports RAID 1, 5 or better	
8	PCI Slots (I/O)	2xPCIe Slots or better	
9	NIC ports	Minimum 4x1G ports	
10	HBA ports	Minimum 2 X 8/16G FC ports	
11	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12	Out-of-Band	Must Support 1G Out of Band connectivity	
13	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	

14	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
15	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management & system health	
16	Warranty	As per RFP requirement	

B.8	Server/Workstation for Baggage Scanner System		
S.No	Paramter	Specification	Compliance (Yes/ No)
1	Rack Height	4U or lower	
2	CPU Support	Must support 2 CPU's	
3	Processors	minimum 2 processor with 16 Cores or better	
4	Processor Clock Speed	2.5GHz or better	
5	Memory	Minimum 64GB RAM per server	
6	Hard Drives	Minimum 2 X 600GB SAS drives, 4 X 1TB SAS 7200 RPM	
7	RAID Card	RAID Controller Card supports RAID 1, 5 or better	
8	PCI Slots (I/O)	2xPCIe Slots or better	
9	NIC ports	Minimum 4x1G ports	
10	HBA ports	Minimum 2 X 8/16G FC ports	
11	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12	Out-of-Band	Must Support 1G Out of Band connectivity	
13	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	
14	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
15	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management & system health	
16	Warranty	As per RFP requirement	

14. Access Control System Server- Technical Compliance			
B.9	Server/Workstation for Backup Solution		
S.No	Paramter	Specification	Compliance (Yes/ No)
1	Rack Height	4U or lower	
2	CPU Support	Must support 2 CPU's	
3	Processors	32 Cores or better	
4	Processor Clock Speed	2.5GHz or better	
5	Memory	Minimum 64GB RAM per server	
6	Hard Drives	Minimum 2 X 600GB SAS drives	

7	RAID Card	RAID Controller Card supports RAID 1, 5 or better	
8	PCI Slots (I/O)	2xPCIe Slots or better	
9	NIC ports	Minimum 4x1G ports	
10	HBA ports	Minimum 2 X 8/16G FC ports	
11	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12	Out-of-Band	Must Support 1G Out of Band connectivity	
13	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	
14	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
15	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management & system health	
16	Warranty	As per RFP requirement	

B.10	PC Workstation		
S.No	Parameter	Specification	Compliance
1.	Form Factor	Tower	
2.	Processor	i7 / Ryzen 7	
3.	Operating System	Windows 10 Pro, 64bit or latest	
4.	Office	Microsoft office standard edition latest.	
5.	Chipset	Intel Workstation Chipset 400 Series or higher	
6.	Memory	32GB in combination of (4x8GB) DDR42666MHz Memory or higher	
7.	Hard Drive	256GB SSD and HDD 1TB	
8.	Graphic Card	Yes	
9.	Keyboard & Mouse	Wired Keyboard & Mouse	
10.	Monitor	Should be able to support video-wall	
11.	PSU	80PLUS Gold Certified Energy Star Compliant	
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
13.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
14.	I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector	
15.	Warranty	As mentioned in RFP	

B.11	**Storage System**

S.No	Parameter	Specification	Compliance (Yes/ No)
1	Storage	Storage Capacity should be a minimum of 2.5 PB Or more as per solution /operation/tender requirement.	
		RAID solution offered must protect against double-disc failure. Or better	
		To store all types of data (Data, Voice, Images, Video, etc.). Storage system capable of scaling vertically or horizontally or Better or Equivalent	
2	Drive Composition	The storage must be configured with at least 20% SSD, and 80% NL-SAS or better as per solution requirements	
		The storage should support multiple drive types like SSD, SAS and NL-SAS Drives. Should support automatic data tiering of data between these 3 drive types depending on the access pattern.	
3	Hardware Platform	Rack-mounted form-factor. Modular design to support controllers and disk drives expansion	
4	Controllers	At least 2 or more Controllers shall be in active/active mode. The controllers / Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for performance, capacity enhancement, and software/firmware upgrades or better as per solution /operation/tender requirement.	
5	RAID support	RAID 5 or 6 or Better	
6	Cache	Minimum 256 GB of useable cache across all controllers or better	
7	Redundancy and High Availability	The Storage System should be able to protect the data against a single point of failure concerning hard disks, connectivity interfaces, fans, and power supplies or any other equipment redundancy required.	
8	Management software	1. All the necessary software (GUI Based) to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots, etc. are to be provided for the entire system proposed. Or better. 2. Licenses for the storage management software should include disc capacity/count of the complete solution and any additional disks to be plugged in in the future, up to the max capacity of the existing controller/units. 3. A single command console for the entire storage system. Or better	
		Should also include storage performance monitoring and management software	
		Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures	
		Should be able to take "snapshots" of the stored data to another logical drive for backup purposes	
		The proposed storage should be configured with Hardware Controller Based Data at Rest Encryption with no dependency on any software or any drive type	
9	Backup Software	To be provide by bidder as per solution requirement	
10	License	**All licenses/ software should be licensed for entire capacity of the supplied array**	

C.1	Access switch 16 Port Non-POE	
S. No.	Specifications	Compliance
1	Minimum 16 x 10/100/1000 and 2 x 1/10G ports (with required transceiver modules)	
2	Switch should 36Gbps or higher Backplane capacity	
3	Switch should support minimum 26 Mpps of forwarding rate	
4	Should support Non-blocking hardware architecture	
5	Support for at least 1000 VLANs & 16k MAC address	
6	It should support IGMP snooping v1,v2 & v3	
7	Switch should support 8 hardware queues per port	
8	Dynamic Host Configuration Protocol (DHCP) snooping	
9	Switch should support LLDP capabilities	
10	Should support IP Source Guard, DAI and IPv6 Security feature like IPv6 RA Guard and IPv6 Neighbour Discovery Inspection	
11	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).	
12	Switch needs to have console port for administration & management	
13	Management using CLI, GUI using Web interface should be supported	
14	FTP/TFTP for upgrading the operating System	
15	Switch should support internal redundant power supply and Hotswappable fans	

C.2	Access switch 24 Port Non-POE	
S. No.	Specifications	Compliance
1	Minimum 24 x 10/100/1000 and 4 x 10G ports (with required transceiver modules)	
2	1 U Rack mountable	
3	The Switch should have minimum 2GB DRAM and 4GB internal Flash/ SSD	
4	128Gbps or higher Backplane capacity and minimum 95 Mpps of forwarding rate (excluding the stacking bandwidth and forwarding)	
5	Should support Non-blocking hardware architecture	
6	Support for at least 4000 VLANs & 16k MAC address	
7	It should support IGMP snooping v1,v2 & v3	
8	It should have static IP routing from Day 1 and should be upgradable to support OSPF, PIM, VxLAN and BGP	
9	The switch should support minimum 10k IPv4/ 1K IPv6 and 1k Multicast Routes	
10	Switch should support 8 hardware queues per port	

11	Dynamic Host Configuration Protocol (DHCP) snooping	
12	Switch should support LLDP capabilities	
13	Should support IP Source Guard, DAI and IPv6 Security feature like IPv6 RA Guard and IPv6 Neighbor Discovery Inspection	
14	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).	
15	Switch needs to have console port for administration & management	
16	Management using CLI, GUI using Web interface should be supported	
17	FTP/TFTP for upgrading the operating System	
18	Switch should support IEEE 802.1ae MACsec (AES-256) on uplink ports	
19	Switch should support internal redundant power supply and Hotswappable fans	

C.3	Access switch 48 Port Non POE	
S. No.	Specifications	Compliance
1	Minimum 48 x 10/100/1000 and 4 x 10G ports (with required transceiver modules)	
2	1 U Rack mountable	
3	The Switch should have minimum 2GB DRAM and 4GB internal Flash/ SSD	
4	176Gbps or higher Backplane capacity and minimum 130Mpps of forwarding rate (excluding the stacking bandwidth and forwarding)	
5	Should support Non-blocking hardware architecture	
6	Support for at least 4000 VLANs & 16k MAC address	
7	It should support IGMP snooping v1,v2 & v3	
8	It should have static IP routing from Day 1 and should be upgradable to support OSPF, PIM, VxLAN and BGP	
9	The switch should support minimum 10k IPv4/ 1K IPv6 and 1k Multicast Routes	
10	Switch should support 8 hardware queues per port	
11	Dynamic Host Configuration Protocol (DHCP) snooping	
12	Switch should support LLDP capabilities	
13	Should support IP Source Guard, DAI and IPv6 Security feature like IPv6 RA Guard and IPv6 Neighbor Discovery Inspection	
14	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).	
15	Switch needs to have console port for administration & management	
16	Management using CLI, GUI using Web interface should be supported	
17	FTP/TFTP for upgrading the operating System	

18	Switch should support IEEE 802.1ae MACsec (AES-128/256) on uplink ports	
19	Switch should support internal redundant power supply and Hotswappable fans	

C.4	Industrial Grade 8 Port POE+ Switch	
S. No.	Specifications	Compliance
1	Minimum 8 x 10/100/1000 and 2 x 1G ports (with required transceiver modules)	
2	Forwarding Rate- Wire speed for all the ports	
3	Should support PoE+ as per IEEE 802.3at or 802.3bt with PoE budget of 240w	
4	Switch should support minimum 4 priority queues	
5	Should support following layer 2 features STP, RSTP, MSTP, IGMP query solicitation IGMP snooping (IGMPv1, v2 and v3) IGMP snooping fast-leave IGMP/MLD multicast forwarding (IGMP/MLD proxy) MLD snooping (MLDv1 and v2)	
6	Switch should support minimum 1K IGMP groups	
7	Switch should support 8K MAC Table size	
8	Should support ACLs, DHCP snooping, IP source guard and Dynamic ARP Inspection (DAI),	
9	Should support MAC address filtering and MAC address lock-down, IEEE 802.1x, DHCPv4 snooping, RSPAN/Port Mirroring	
10	MAC and 802.1 X based Login must be available	
11	Switch should support following management features: - CLI, GUI, SNMPv1, v2c and v3, RMON MIB	
12	Switch should support -20C to 60C operating temperature, Humidity: 5% to 95% non-condensing IP30 Rating	

C.5	Distribution Switch	
S. No.	Specifications	Compliance (Yes / No)
A. Solution Requirement		
1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	

2	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 inbuilt level of redundancy	
B. Hardware and Interface Requirement		
1	The switch should have 48 x 1/10/25G and 6 x 40/100G Uplink Ports	
2	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 inbuilt level of redundancy	
3	Switch should have minimum 8GB DRAM and 8GB internal Flash/Storage	
4	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG , EVPN LAG .etc.	
5	The switch should support minimum 200,000 IPv4 unicast routes and 100,000 IPv6 unicast routes entries in the routing table including 48,000 multicast routes	
6	The switch should support hardware based load sharing at wire speed using LACP and multi chassis ether channel/LAG	
7	Switch should have non-blocking architecture with 3.6 Tbps switching capacity and 2.5 bpps or more forwarding rate	
C. Layer2 Features		
1	Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S)	
2	Switch should support minimum 200,000 no. of MAC addresses	
3	Switch should support minimum 8 Nos. of link or more per Port channel (using LACP) and support 48 number of ports per Link Aggregation Group. The Switch should support 32 way ECMP	
4	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
D. Layer3 Features		
1	Switch should support static and dynamic routing like Static, OSPF and BGP	
2	Should support BGP, MBGP, IS-IS for IPv4 and IPv6	
3	Switch should support multicast traffic reachability using PIM-SM and SSM	
E. Availability		
1	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/ VRRP	
2	Switch should support for BFD For Fast Failure Detection	
F. Quality of Service		
1	Switch system should support 802.1P classification and marking of packet CoS, DSCP etc.	
2	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	
G. Security		

1	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V4 and IP V6 and logging for fault finding and audit trail	
2	Switch should support for external database for AAA using TACACS+ / Radius	
3	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
H. Manageability		
1	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	
2	Switch should provide remote login for administration Telnet, SSHv2	
3	Switch should support for management and monitoring status using different type of Industry standard NMS using SNMP V2 and V3	
4	Switch should support for basic administrative tools like Ping and traceroute	
5	Switch should support central time server synchronization using Network Time Protocol NTP V4	

C.6	Access switch 16 - PoE+	
S. No.	Specifications	Compliance
1	Minimum 16 x 10/100/1000 PoE+ and 2 x 1/10G ports (with required transceiver modules)	
2	Switch should have a minimum power budget of 240W	
3	Switch should provide 36Gbps or higher Backplane capacity	
4	Switch should support minimum 26 Mpps of forwarding rate	
5	Should support Non-blocking hardware architecture	
6	Support for at least 1000 VLANs & 16k MAC address	
7	It should support IGMP snooping v1,v2 & v3	
8	Switch should support 8 hardware queues per port	
9	Dynamic Host Configuration Protocol (DHCP) snooping	
10	Switch should support LLDP capabilities	
11	Should support IP Source Guard, DAI and IPv6 Security feature like IPv6 RA Guard and IPv6 Neighbor Discovery Inspection	
12	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).	
13	Switch needs to have console port for administration & management	
14	Management using CLI, GUI using Web interface should be supported	
15	FTP/TFTP for upgrading the operating System	
16	Switch should support internal redundant power supply and Hotswappable fans	

C.7	Access switch 24 - PoE +	
S. No.	Specifications	Compliance
1	Minimum 24 x 10/100/1000 PoE+ and 4 x 10G ports (with required transceiver modules) with PoE budget of minimum 720W	
2	1 U Rack mountable	
3	The Switch should have minimum 2GB DRAM and 4GB internal Flash/ SSD	
4	128Gbps or higher Backplane capacity and minimum 95 Mpps of forwarding rate	
5	Should support Non-blocking hardware architecture	
6	Support for at least 4000 VLANs & 16k MAC address	
7	It should support IGMP snooping v1,v2 & v3	
8	It should have static IP routing from Day 1 and should be upgradable to support OSPF, PIM, VxLAN and BGP	
9	The switch should support minimum 10k IPv4/ 1K IPv6 and 1k Multicast Routes	
10	Switch should support 8 hardware queues per port	
11	Dynamic Host Configuration Protocol (DHCP) snooping	
12	Switch should support LLDP capabilities	
13	Should support IP Source Guard, DAI and IPv6 Security feature like IPv6 RA Guard and IPv6 Neighbor Discovery Inspection	
14	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).	
15	Switch needs to have console port for administration & management	
16	Management using CLI, GUI using Web interface should be supported	
17	FTP/TFTP for upgrading the operating System	
18	Switch should support IEEE 802.1ae MACsec (AES-256) on uplink ports	
19	Switch should support internal redundant power supply and Hotswappable fans	

C.8	Access switch 48 - PoE +	
S. No.	Specifications	Compliance
1	Minimum 48 x 10/100/1000 and 4 x 10G ports (with required transceiver modules) with PoE budget of minimum 1440W	
2	1 U Rack mountable	
3	The Switch should have minimum 2GB DRAM and 4GB internal Flash/ SSD	
4	176Gbps or higher Backplane capacity and minimum 130Mpps of forwarding rate	
5	Should support Non-blocking hardware architecture	
6	Support for at least 4000 VLANs & 16k MAC address	
7	It should support IGMP snooping v1,v2 & v3	
8	It should have static IP routing from Day 1 and should be upgradable to support OSPF, PIM, VxLAN and BGP	
9	The switch should support minimum 10k IPv4/ 1K IPv6 and 1k Multicast Routes	
10	Switch should support 8 hardware queues per port	
11	Dynamic Host Configuration Protocol (DHCP) snooping	
12	Switch should support LLDP capabilities	

13	Should support IP Source Guard, DAI and IPv6 Security feature like IPv6 RA Guard and IPv6 Neighbor Discovery Inspection	
14	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).	
15	Switch needs to have console port for administration & management	
16	Management using CLI, GUI using Web interface should be supported	
17	FTP/TFTP for upgrading the operating System	
18	Switch should support IEEE 802.1ae MACsec (AES-128/256) on uplink ports	
19	Switch should support internal redundant power supply and Hotswappable fans	

C.9	Distribution Switch 48 port	
S. No.	Specifications	Compliance (Yes / No)
A. Solution Requirement		
1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
2	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 inbuilt level of redundancy	
B. Hardware and Interface Requirement		
1	The switch should have 48 x 1/10/25G and 6 x 40/100G Uplink Ports	
2	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 inbuilt level of redundancy	
3	Switch should have minimum 8GB DRAM and 8GB internal Flash/Storage	
4	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG , EVPN LAG .etc.	
5	The switch should support minimum 200,000 IPv4 unicast routes and 100,000 IPv6 unicast routes entries in the routing table including 48,000 multicast routes	
6	The switch should support hardware based load sharing at wire speed using LACP and multi chassis ether channel/LAG	
7	Switch should have non-blocking architecture with 3.6 Tbps switching capacity and 2.5 bpps or more forwarding rate	
C. Layer2 Features		
1	Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S)	
2	Switch should support minimum 200,000 no. of MAC addresses	

3	Switch should support minimum 8 Nos. of link or more per Port channel (using LACP) and support 48 number of ports per Link Aggregation Group. The Switch should support 32 way ECMP	
4	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
D. Layer3 Features		
1	Switch should support static and dynamic routing like Static, OSPF and BGP	
2	Should support BGP, MBGP, IS-IS for IPv4 and IPv6	
3	Switch should support multicast traffic reachability using PIM-SM and SSM	
E. Availability		
1	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/ VRRP	
2	Switch should support for BFD For Fast Failure Detection	
F. Quality of Service		
1	Switch system should support 802.1P classification and marking of packet CoS, DSCP etc.	
2	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	
G. Security		
1	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V4 and IP V6 and logging for fault finding and audit trail	
2	Switch should support for external database for AAA using TACACS+ / Radius	
3	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
H. Manageability		
1	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	
2	Switch should provide remote login for administration Telnet, SSHv2	
3	Switch should support for management and monitoring status using different type of Industry standard NMS using SNMP V2 and V3	
4	Switch should support for basic administrative tools like Ping and traceroute	
5	Switch should support central time server synchronization using Network Time Protocol NTP V4	

C.10	Core Switch		
S.No	Parameter	Description	Compliance (Yes / No)
1	Type	Should be Modular chassis-based Switch with at least 4 Slots for line cards and with dual redundant CPU/Switch fabric and redundant power supply. In the event of failure of one one CPU/Switch fabric/routing engine, forwarding should not stop and failover from one CPU/Switch fabric/routing engine to other should be stateful	
2	Ports	minimum 32 x 40/100G Ports	
		Minimum 30 x 10G/25G Ports	
3	Switching and Forwarding capacity	Aggregate capacity of minimum 7.9Tbps or more and minimum 5.99Bpps or more Forwarding Rate The switch architecture should be non-blocking for its switching capacity and forwarding bandwidth.	
4	Per slot bandwidth	Min 1.2Tbps	
		Should support Redundant CPU	
		Redundant Power Supplies from Day 1	
		Support 100G and 400G from Day 1	
		Support for Hot Swap of redundant components like Power Supply, and fan trays	
		Should support ESI-LAG/ MC-LAG/ vPC/ MLAG	
5	Memory and Storage	16 GB DRAM and 64GB Flash/ SSD	
6	Layer 2 features	Should support Industry Standard Port/Link Aggregation for All Ports.	
		Jumbo Frames support up to 9K Bytes	
		Should support port, subnet based 802.1Q VLANs. The switch should support minimum 4,000 vlans	
		The switch should support minimum 150,000 no. of MAC addresses.	
		The switch should support IEEE 802.1w RSTP and IEEE 802.1s MSTP	
7	Routing Protocols	Should have RIP, OSPF v1/v2, BGPv4, IS-IS, EVPN/ VxLAN from Day 1	
		Should support minimum 500,000 IPv4 routes	
8	Security features	Should Support MAC Address Filtering based on source and destination address	
		Should have support for RADIUS and TACACS+	

		Switch should support MACsec on QSFP28 and SFP+ports	
9	Traffic policing	Should support Ingress/Egress Queuing	
		Should be able to filter, mark and limit traffic flows	
		Should support policy based traffic classification based on Type of Service (ToS), IP Precedence mapping, Layer 2/3/4 defined traffic flows, MAC address, VLANs	
		Should Support IGMP v1, v2 and IGMP Snooping/ filtering	
10	Network monitoring /management	Should Support SNMP, RMON/RMON-II, SSH, telnet, web management through network management software (NMS/ EMS)	
		Should support port mirroring feature for monitoring network traffic.	
		The switch should support role based access control to limit access to switch operations.	

C.11	Wi-Fi Access Point - Indoor	
S.No	Description	Compliance
1	The Access Point should support 802.11ax wifi-6/6E standard	
2	The solution must support 2.4GHz, 5GHz ,6GHz bands.	
3	The solution Should have Bluetooth 5.1 support	
4	The solution Should have minimum 1x 100M/1000M/2.5G Multigigabit Ethernet (RJ-45), USB Port.	
5	The solution Should support MU-MIMO technology	
6	The Minimum Peak combined datarate should be 7Gbps.	
7	The solution Should have option to create multiple SSIDs.	
8	The solution should have Mechanism for physical device locking using padlock / Kensington lock or equivalent	
9	The solution Should have mounting option of ceiling/wall/T-Rail.	
10	Access point should support below minimum Wireless Monitoring Capabilities	
	a) Rogue Scan detection for Ap	
	b) WIPS / WIDS support	
11	Access point Operating Temperature should be: 0° to 50°C	
12	The access point must support WPA2/WPA3 enterprise authentication and AES encryption.	
13	The solution Should support Power over Ethernet	
14	The solution should be able to integrate with various authentication mechanism including radius servers etc.	
15	Should be IPv4 & IPv6 ready from day one	

C.12	Wi-Fi Access Point - Outdoor	
S.No	Description	Compliance
1	The Access Point should support 802.11ax wifi-6 standard	
2	The solution should support minimum dual band.	

3	The solution should have minimum 1x 100/1000/2500 BASE-T, ,1x Gigabit Ethernet SFP	
4	The solution should have wave 2 or higher standards.	
5	The Minimum Peak combined data rate should be more than 5 Gbps.	
6	The solution Should have minimum 2 number of wifi radios	
7	The solution Should have option to create multiple SSIDs.	
8	The solution should have Mechanism for physical device locking using padlock / Kensington lock or equivalent	
9	The solution Should have mounting option of ceiling/wall/T-Rail.	
10	Access point should support below minimum Wireless Monitoring Capabilities	
	a) Rogue Scan Detection	
	b) WIPS / WIDS support	
11	Access point Operating Temperature should be -40 to +60°C	
12	Wifi AP should be ruggedised device and should be in compliance with IP67 standards	
13	Should be IPv4 & IPv6 ready from day one	

C.13	Wi-Fi- Controller	
S.No	Description	Compliance
1	Controller appliance should be Rack mountable hardware controller.	
2	WLC must be compliant with IEEE CAPWAP or equivalent for controller-based Wireless LANs (WLANs). Should have throughtput of minimum 60 Gbps	
3	The solution Should have minimum 4x 10G SFP+/SFP	
4	The solution Should support minimum 2000 access points in a single controller and should be scalable upto 5000 Access points.	
5	The WIPS solution should identify if somebody try to spoof mac address of client or AP for unauthorized authentication.	
6	the solution should support guest portal	
7	The solution should be able to integrate with various authentication mechanism including radius servers etc.	
8	The solution Should support centralized mode.	
9	The solution should support DTLS/TTLS encryption or equivalent to ensure full-line-rate encryption between access points and controller across remote WAN/LAN links.	
10	The solution should support web based management and SSH	
11	Should be a standalone appliance in High Availability mode.	
13	Should support multiple redundancy models like 1+1 and N+1	
14	Should have redundant power supplies.	
15	Must support an ability to dynamically adjust channel and power settings based on the RF environment.	
16	Radio coverage algorithm must allow adjacent WAPs to operate on different channels, in order to maximize available bandwidth and avoid interference	
17	Must support interference detection and avoidance.	
18	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis	
19	Must support RF Management with different available channels	

20	Should support Wireless IEEE standards such as 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave 1 and Wave 2, 802.11ax, etc.	
21	Should support routing and switching IEEE standards such as 802.3, 10Base-T, 802.3u, 100Base-TX, 1000Base-SX, 1000Base-LH, IEEE802.1Q VLAN tagging, IEEE 802..1AX Link aggregation, etc.	
22	Should support data standards such as UDP, IP, IPv6, ICMP, TCP, ARP, CIDR, DHCP, CAPWAP, etc.	
23	WLC Should support unauthorized/Rogue AP detection, classification and standard WIPS Signatures and should be able to detect, locate, mitigate, and contain wired and wireless rogues and threats.	
24	Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, WPA3, Wired Equivalent Privacy (WEP), 802.1X with multiple Extensible Authentication Protocol (EAP) types, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunnel TLS (EAP-TTLS), DTLS	
25	Must support Access Control Lists (ACLs).	
26	Must support built-in web authentication	
27	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.	
28	Must support user load balancing across Access Points.	
29	Must provide Mesh capability for Mesh supported AP	
30	Must be able to dedicate some WAPs to monitor-only for Intrusion Prevention Services.	
31	Must support client roaming across controllers separated by a layer 3 routed boundary.	
32	Must support WAP over-the-air packet capture for export to a tool such as Wireshark / equivalent	
33	Should support the ability to schedule WAP power on/off for energy savings.	
34	Should be able to classify different types of interference within 5 to 30 seconds.	
35	Should support 802.11e WMM	
36	Support for configuring media streams with different priority to identify specific video streams for preferential quality-of-service treatment.	
37	Should support IPv4 & IPv6 from day one.	

C.14	Router	
S. No.	Specifications	Compliance
1	The Router should be fixed / chassis based and 19" rack mountable	
2	The Router should have minimum 16GB RAM	
3	The Router should have Redundant Power Supply and redundant fans	

4	The Router should support minimum 8 x 1/10G Gig fiber interfaces , minimum 2 x 40 Interfaces from Day 1. Router should be capable of supporting additional 6 X 1/10G interface for future scalability .	
5	The Router should support the following:	
	OSPF, BGP, IS-IS, IP Multicast, PIM, IGMP, MLDv2, MPLS, L2VPN, L3VPN, Segment Routing, BGP-LS/LU, VPLS, RSVP, BFD for IPv4 and IPv6.	
6	The Router should have 128k IPv4, 64K IPv6, 8K Multicast routes, 200k MAC and 1000 L2 VPN, 5 label stack depth	
7	The Router should have Protection against Broadcast, Multicast and Unicast Storm.	
8	The Router should support the following features: 802.1Q, LFA, VLAN Stacking (Q-in-Q), Y.1731, 802.1ag, ERPS-G.8032, FRR, LACP, EVPN, HQoS etc.	
9	SSH, NETCONF, Telemetry, and Role based privileges for the system access.	
10	Operating Temperature 0 to + 40 degrees, Relative Humidity: 10% to 85% non-condensing.	

C.15	Network Access Controller (NAC)	
S.No	Description	Compliance
	General Specifications	
1	NAC solution must be best in class fully out-of-band model, deployed and managed centrally with flexible integration options for wired, wireless and VPN infrastructure. It should not be based on SPAN port integration.	
2	License should be perpetual model. The system must support a minimum of 5,000 concurrent devices/users. Licenses are to be applied to currently connected devices/users and to be released when the device is disconnected. The same system should scale upto 15,000 ports without adding any additional hardware or software. Bidder can include 20% of additional license if the nac is not releasing the license when the devices disconnected.	
3	Must offer Network Visibility, Device Profiling, Easy and powerful Onboarding process, Endpoint Compliance, Network Provisioning and Threat Identification module provide security actions through integration.	
4	NAC solution can be deployed in virtual machines VMWare, Hyper-V, AWS, Azure or on hardware appliances.	
5	Must authorize access via VLAN assignment and/or applying access control lists (ACLs).	
6	NAC should be capable to block the access of endpoints which are connected on unmanaged network (i.e Unmanaged Switch) and Managed Network (i.e. Managed Switch).	
7	The proposed solution must be capable of working with endpoint agents and agentless.	
	Endpoint profiling	

8	NAC solution must have the ability to get inventory all all devices on a network and profileing for non-PC equipment like printers, smart phones, IP-phones, and appliances.	
9	Must support profiling for Client and clientless devices based on a DHCP fingerprint, Netflow, Vendor OUI, location,IP range, HTTP/HTTPS, Network traffic, etc	
10	Must support Script based Device Profiling method to execute the command line scripts to profile the device.	
11	The system must collect detailed asset information about MAC address, Logged on user, OS, NIC vendor, Switch Port, etc.,	
	Authentication and Enforcement Requirements:	
12	The solution should allow only authenticated/managed devices to connect to organization networks and enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention.	
13	Must support flexible authentication options to include, Web Authentication and MAC Authentication	
14	Must support MAC-address whitelisting & blacklisting natively	
15	LDAP — Microsoft Active Directory, OpenLDAP, Google SSO	
16	Should be able to append additional attributes to incorporate the authenticator's location, device type, vendor etc apart from the user attributes.	
	Endpoint Compliance and Remediation Requirements	
17	The solution must support both agent-based (Persistent Agent, Dissolvable Agent) and agentless endpoint inspection.	
18	NAC solution must perform system checks on service packs, Domain Verification, Certificate check, patches, critical updates enabled, Antivirus, services/processes running, invalid services/processes, file existence, any Microsoft registry settings.	
19	IT should have an option to create custom scan for monitoring all the service and process scan with schedule time.	
20	Proposed solution must be able to Disable Internet connection sharing, Detect Network bridgres and Trigger SCCM Evaluation	
Guest Management		
21	Guest Management should support notification by SMS and email. It should support Mail to SMS, API, HTTPS-based SMS gateway integration.	
22	Must support Customization of SMS and E-Mail messages for Self-Registered and Pre-Registered Guests	
23	Guest Management should be configurable to meet various requirements such as short or long-term guests, conference mode or self-registered guest	
24	Solution should support limited and controlled administrative access for Guest Management Only.	
25	NAC must have an option to create separate portals pages for different sets of users based on host connection location, IPaddress, MAC Address, Operating System.	
26	Guest Management should support employee sponsorship workflow.	
27	Must support API integration with the various Social Media sites Facebook, Google, LinkedIn, Outlook, Twitter and Yahoo.	
AAA		

28	The solution should be Dedicated redundant Hardware Appliances. Should be supplied with 5000 license scalable upto 15000	
29	The solution Should be able to integrate with all makes of manageable network devices which are capable of supporting open standards-based protocols required for NAC operation	
30	The solution Must provide Network Access Control and visibility in single pane of glass for the entire infrastructure from day 1 spread across multiple Network Locations / Zones	
31	The solution Must allow system-level operations such as device discovery, event management, logging and application maintenance to be performed centrally.	
32	The solution must provide the capabilities to modify, filter, and create your own flexible views of the network.	
33	The solution Must support RADIUS and LDAP Authentication for users/devices of the application.	
34	When integrated with security devices such as IDS it must be able to isolate and quarantine the attacker without disruption to other users, applications and business critical systems	
35	Must provide a web interface that contains reporting, dashboards, troubleshooting and monitoring tools.	
36	The solution Must provide port level analysis capability	
37	The solution Must provide customizable reports	
38	The Solution should have capability to integrate with IoT solutions	
39	The Should have the capability to integrate with 3rd party vendors	
40	If required, solution should be deployable in a distributed mode with different units for Different Locations for ease of management, Authorization and Policy Control. All individual Units should be integrated to one central Control Unit with hierarchical management access or role-based access like admin, operator etc.	
41	The Solution must utilize standards-based authentication mechanisms enabling non-intelligent devices the ability to connect to the network and receive the proper network services.	
42	Detect and protect any device with IP address without the need for a client application on each endpoint including detection of VoIP phones, printers, wireless devices, machinery, cameras, sensors etc.	
43	The solution should Support event logging of Device Access and Activity Time Stamp	
44	Device search functionality by attributes such as user name / OS type / IP- MAC address / System Name	
45	Must support automated onboarding and self-registration of all IP end points. Must also offer the option of sponsorship capabilities to validate guest registration without involvement of IT staff.	
46	Must Support location-based Registration portals to redirect Users entering through common location to different portals for different Network Zones	
47	Must support automated context-based policy provisioning of network services for mobile devices	
48	Solution must support User Validation as well as device Validation for two factor security against an AD or LDAP database. Support integration with multiple LDAP / AD servers	

49	Ipv6 support for NAC implementation in networks with Ipv6 end systems-preferred.	
50	Support Management Access Authentication and Authorization for Network Device Access	
51	Support Manipulation of Radius Attributes for Authentication as well as Radius Accept	
52	Must be able to create correlated topology based on LLDP, SNMP, L2 and L3 protocol connectivity hierarchy	
53	Must allow system-level operations such as device discovery, event management, logging and application maintenance to be performed centrally.	
54	Must support RADIUS or LDAP Authentication for users of the application.	
55	Must provide a tool to search and locate the physical location of connected devices and end users, quickly and easily.	
56	Must allow IT administrators to easily define a number of pre- configured network policies, and designate select personnel to activate/deactivate these policies as appropriate	
57	Must provide capability to bind together the username, IP address and MAC ad- dress, and physical port of each endpoint for forensic analysis	
58	Must provide an interface with troubleshooting and monitoring tools (Ping / Traceroute, SSH, Telnet, Http/s)	
59	Must provide event logs for the entire infrastructure of Network devices	
60	Must provide user customizable reports creation	
61	Must be able to interact with network security devices and push template based automated response to security events and thus remediating real time threats	
62	Must provide open XML APIs for integration with third party applications.	
63	Must support the ability to monitor end-system events and view the health results from an end-system's latest assessment scan.	
64	Must provide easy-to-use dashboards and detailed views of the health of the end systems attached or trying to attach to the network.	
65	Must provide the ability for analysts to be able to easily tailor the dashboard views to present the information in their preferred format.	
66	Should be capable of reporting for historical and real-time data. Should be equipped with Custom report designer to meet the needs of specific data attributes and periodic email of the same to relevant Administrative team.	
67	VLAN steering and port bouncing via SNMP/RADIUS	
68	Ability to perform caching of MAC address post guest authentication to avoid the need for guest to re-authenticate during the period of their visit (3G like user experience after first authentication via captive portal).	
69	Policy model should support incorporation of several contextual elements including identity, endpoint health, device, authentication method & types, and conditions such as location, time, day, etc.	
70	AAA framework must allow for the complete Authentication and Authorization sources from databases (like AD/LDAP/RADIUS/TACACS).	
71	All external facing interfaces are programmable, which means APIs are available to extend the system to support different authentication protocols, identity stores, health evaluation engines and port and vulnerability scanning engines.	

72	The solution Must be an easy-to-deploy hardware platform that utilizes identity-based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform:	
73	• Built-in guest management and device/user onboarding	
74	• Web based management interface with Dashboard	
75	• Reporting and analysis with custom data filters	
76	• Data repository for user, device, transaction information	
77	• Rich policies using identity, device, health, or conditional elements	
78	• Deployment and implementation tools.	
79	Must support flexible licensing model based on required functionality (i.e. Profile, Onboard, Guest Access).	
80	Correlation of user, device, and authentication information for easier troubleshooting, tracking etc.	
81	Platform must be deployable in an out-of-band model and support for clustering with N+1 redundancy model.	
82	Flexibility to operate all features/functions on any appliance in the cluster.	
83	Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.	
84	Support any type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1X, MAC auth, Web auth).	
85	Ability to take advantage of a phased implementation approach by starting with one element of access management (role based) and later incorporating added security measures (endpoint health).	
86	Must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together.	
87	Agent-based enforcement – bouncing a managed interface and sending custom messages. Also, control access to different networks via whitelist and blacklist. License as per requirement.	
88	Must be able to join multiple Active Directory domains to facilitate authentication.	
89	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform & SIEM.	
90	**should provide an easy-to-use BYOD ready granular secure access control solution that is context aware, identity enabled, location and device based.**	
91	**must be deployed with 802.1x authentication for managed endpoints to provide Zero Trust Security with Pre- and Post-Admission Control; alternate authentication methods such as MAC address authentication or web authentication to authenticate endpoint devices that do not support 802.1X authentication**	
92	**must be vendor agnostic and support heterogeneous environment**	
93	**must support network-based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility**	
94	**must provide flexible filtering capabilities to sort out device information based on different attributes (e.g. MAC address, Manufacturer name, hostname, IP address, etc.)**	

95	**must have built-in/separate Anomaly detection and Behavioral analytics capability**	
96	**should integrate with multivendor Switches and Wireless Controllers to support enforcement actions**	
97	**should support posture assessment capabilities on Windows, MaC & Linux endpoints**	
98	**should be able to integrate with firewall and perform Layer 3 enforcement to secure applications and services from unauthorized access.**	
99	**should be able to perform Layer 2 enforcement at the network layer by integrating with network switches and wireless solution**	
100	should have monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations	

C.16	SAN Switch		
S.No	Parameter	Description	Compliance
1	Switch Architecture	The SAN switch shall support nonblocking architecture with minimum 48*16G/32G FC active ports with full duplex in single domain with no oversubscription and all ports on the supplied FC SAN switch must be licensed and should be fully populated from day one.	
3	Autosensing capabilities	The proposed ports should have autosensing capabilities to 32/16/8 Gbps FC connectivity	
4	Trunking capabilities	The switch should support trunking with up to eight 32 Gbps ports per ISL trunk	
5	Performance	Should support aggregate bandwidth of minimum of 768 Gbps or higher	
6	Port Types supported	Should support D_PORT (Clear Link Diagnostic Port), E_PORT, EX_PORT, F_PORT, AE_PORT	
7	Media/Transceiver Types	Should support hot-pluggable Fiber Channel SFP+ at 32 Gbps SWL/LWL and SFP+ at 16 Gbps SWL/LWL/ELWL	
8	USB Port	Should have at least One USB port per control processor for firmware download, support save, and configuration upload or download	
9	Management	Should have switch management feature with support for e HTTP, SNMP v1/v3 (FE MIB, FC Management MIB), SSH; Auditing, Syslog; Command Line Interface (CLI); SMI-S compliant	

10	Security	Should support DH-CHAP (between switches and end devices), HTTPS, IPsec, IP filtering, LDAP with IPv6, Port Binding, RADIUS, TACACS+, user-defined Role-Based Access Control (RBAC), Secure Copy (SCP), Secure RPC, Secure Syslog, SFTP, SSH v2, SSL, Switch Binding, Trusted Switch	
11	Warranty	As per RFP Requirement	

C.17	WAF	
S.No	Description	Compliance
1	General Requirements:	
a	Web application firewall should be appliance based and provide specialized application threat protection.	
b	Web application firewall should protect web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations.	
c	Should protect against application-level attacks targeted at web applications.	
d	Should provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting,	
e	Should provide controls to prevent identity theft, financial fraud and corporate espionage.	
f	Appliance should have unlimited application licenses.	
g	Automatic signature update and install	
h	Should monitor and enforce government regulations, industry best practices, and internal policies.	
2	Performance requirements	
a	Should support 50,000 HTTP transactions per second	
b	Should support 1M HTTP concurrent connections	
c	Should deliver at least 5 Gbps of WAF (HTTPs) throughput and not the L7 throughput	
d	Interface and connectivity requirements	
e	Should support 4 no's of 10/100/1000 Interfaces and 4 x 10G SFP+ SR Ports. The 1G ports support support internal bypass.	
f	Should support inbuilt 500 GB of Storage space (preferably SSD)	
4	Feature specifications.	
a	The appliance should be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, proxy mode,	
b	Appliance should continuously track the availability of the Servers being protected.	
c	Should have a Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.	
d	Should have Data Leak Prevention module to analyze all outbound traffic alerting/blocking any credit card leakage and information disclosure	

e	Provide controls to meet PCI compliance requirements for web application servers.	
f	Should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.	
g	Should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.	
h	Should support automatic signature updates to protect against known and potential application security threats.	
i	WAF should support fail open in case of hardware failure	
j	Should support custom signatures	
k	Provide ability to allow/deny URL access	
l	Ability to define different policies for different applications	
m	Ability to create custom attack signatures or events	
n	Ability to combine detection and prevention	
o	Should protect certain hidden form fields.	
p	Must provide ability to allow or deny a specific URL access.	
q	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, Converting back slash to forward slash character etc..	
r	For mobile clients that cannot execute Java script or CAPTCHA, the solution should be able to verify the legitimate request by verifying the token a mobile application carries when it access a web server	
s	The solution should be able to protect the Mobile APIs from malicious attacks by verifying the mobile device authenticity	
t	The WAF should support IP Reputation Service and able to provide up to date information about threatening sources.	
u	Support IPv6 for Reverse Proxy deployments and It should also Support IPv4 to IPv6 and IPv6 to IPv4 communication	
v	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests	
w	The solution should be able to support deception technique to identify bots through inserting a hidden link into response page.	
x	The solution should be able to verify bot clients by monitoring events such as mouse movement, keyboard, screen touch, and scroll, etc	
y	The solution should have inbuild Antivirus module for scanning malicious content in file uploads or should be proposed withadditional Antivirus solution to scan the malacious content during file uploads.	
z	The solution should support anomaly detection model to eliminate noise samples and reduce false positives.	
5	Auto Learn	
a	Should have the capability to Auto-Learn Security Profiles required to protect the Infrastructure.	
b	Should provide a statistical view on collected application traffic	
c	Policies must be automatically generated from auto learn results	
d	auto-learn options should be available to tweak and fine tune rules	
e	WAF should continue to provide protection even while in learning mode.	
f	Brute Force Attack	
g	Should have controls against Brute force attacks	
h	should Detect brute force attack (repeated requests for the same resource) against any part of the applications	

i	Custom brute force attack detection for applications that do not return 401.	
j	Protection against SYN-flood type of attacks	
6	Cookie Protection	
a	Should be able to protect Cookie Poisoning and Cookie Tampering.	
b	Strict Protocol Validation	
c	Must support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP1.1	
d	Should support restricting the methods used.	
e	Should support restricting the method exceptions.	
f	Should validate header length, content length, Body length, Parameter length, body line length etc..	
7	SSL	
a	Appliance should be able to terminate SSL	
b	Should Passively decrypt SSL	
c	Client certificates should be supported in passive mode and active mode.	
d	In termination mode, the backend traffic (i.e. the traffic from the WAF to the web server) can be encrypted via SSL	
e	Are all major cipher suites should be supported by the SSL v3 implementation.	
f	Should support for hardware-based SSL acceleration or SSL off loading	
8	High Availability and load balancing	
a	Should support High Availability in active mode,	
b	WAF appliance should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers.	
c	WAF appliance should support Data compression for better response time to users	
9	Vulnerability Scanning.	
a	The product must possess a Web Application Vulnerability Scanning capability built in.	
b	The vulnerability scan should identify vulnerabilities such as XSS, SQL injection, Source code disclosure, Common web server vulnerabilities etc..	
c	Scan must be able to crawl the Web application	
d	Must be able to scan the authenticated applications.	
e	Should support scheduled scanning.	
f	Should support exclusions in scanning by the administrator.	
10	Logging and Reporting.	
a	Ability to identify and notify system faults and loss of performance	
b	Should support Log Aggregation	
c	Should support multiple log formats such as CSV, Syslog, TXT, etc..	
d	Should support inbuilt Reporting and sending the report via E-Mail	
e	Should support report formats in PDF, HTML, WORD, RTF, etc..	
f	Reports should be customizable.	
g	Report Distribution Automatically via email	
h	Should generate comprehensive event reports	
i	Should able to monitor real-time HTTP throughput	

D.1.a	**Software for Video Management**	
S.No	Description	Compliance
A	General	
1	The Video Management System shall be a fully distributed solution, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors. The Video Management System shall offer centralized management of all devices, servers and users and must empower a flexible rule-based system driven by schedules and events.	
2	The VMS application shall support all the features & functionalities of the offered cameras.	
3	To ensure openness, VMS and cameras may not be from the same manufacturer but should be tightly integrated.	
4	VMS shall support installation and ability to run on virtualized environment	
5	VMS manufacturer shall provide their SDK (or any other integration means) libraries and documentation) to ensure a seamless integration with any other system	
6	VMS shall be open to any standard storage technologies integration.	
7	VMS shall be open to any video wall system integration.	
8	VMS should consist of only Base license and Channel Licenses. VMS should be provided with unlimited number of Failover Servers and Failover Camera Licenses , with no dependency of VMS licenses by binding with the MAC address of the cameras to achieve the functionality	
9	VMS should support Scalable Video Quality Recording to record high-quality video to edge storage, while a low-quality reference video stream can be recorded centrally in the recording servers	
10	The VMS system shall be a scalable client – server architecture built using well known operating systems	
11	The VMS system shall enable recording to be done at the aggregation sites and shall allow the local Control centre to import selected video's on demand.	
12	The VMS system shall be compatible to single and multiple processor servers. The server processor & hardware shall be optimized in all cases.	
13	The VMS system shall cluster the processing & memory load across several machines. The failure of any one server in the solution shall not cause a failure in the entire system.	
14	The VMS system device drivers shall be stored separately to the central core application to ensure any instability in 3rd party SDKs do not affect the core application.	
15	The VMS management server shall be able to intelligently scan an IP network for new devices.	

16	The VMS system shall provide an integrated secure, scalable and easily accessible software-based solution for the management of the existing & future physical security infrastructure	
17	The VMS system shall provide a powerful and efficient management interface for all the security systems across all monitored sites.	
18	The Video Management System shall be a fully distributed solution, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors. The Video Management System shall offer centralized management of all devices, servers and users and must empower a flexible rule-based system driven by schedules and events.	
19	The Video Management System shall work on recording servers used for recording video feeds and for communicating with cameras and other devices. The recording servers shall process the recordings and playback the video streams.	
20	The Video Management System shall include a federated architecture allowing clients on the host system with the right user rights to view video sources belonging to multiple independent Video Management Systems simultaneously, as if they were on The Video Management System shall contain a management server that shall be the central manager of the system and control recording servers, cameras, devices and users. The management server shall handle the initial client login, system configuration and logging.	
21	The management server shall allow access to a system manager from where the administrator can configure and manage all servers, cameras and users.	
22	The system shall allow the management server to be installed on multiple servers within a cluster of servers ensuring that another server in the cluster automatically takes over in case the first server fails.	
23	The Video Management System shall support installation and ability to run on virtualized servers.	
24	The Video Management System shall support a versatile rule system including scheduled or event-driven actions with numerous options including support to time profiles.	
25	The Video Management System shall include automatic camera discovery.	
26	The Video Management System shall support archiving for optimizing recorded data storage through unique data storage solutions by combining performance and scalability with cost efficient long-term video storage.	
27	The Video Management System shall incorporate fully integrated matrix functionality for distributed viewing of any camera in the system from any computer with the client viewer.	

28	The Video Management System shall incorporate intuitive map functions allowing for multilayered map environment. The map functionality shall allow for the interactive control of the complete surveillance system, at-a-glance overview of system integrity, and seamless drag-and-drop integration with video wall module option.	
29	The Video Management System shall support full two-way audio between clients and remote devices. Two-way audio integration shall support the following features and functions:	
30	The Video Management System software shall provide fast evidence export by exporting in video to various formats, including video from multiple cameras in encrypted native database format with an included viewer.	
31	The Video Management System shall show full awareness of the system through audit logs and shows user activity through comprehensive logs.	
32	The Video Management System shall include a Software Development Kit (SDK) that offers important capabilities for integrating the Video Management System with third party software and applications.	
33	The Video Management System shall include a stand-alone viewer application to be included with video exported from the client viewer application. The viewer application shall allow recipients of the video to browse and playback the exported video without installing separate software on their computers.	
34	The system shall, after desired retention days, the video feeds will be overwritten unless it is flagged or marked by the authorities for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident in question can be stored locally and/or centrally until the authorities deem it good for deletion.	
35	The Video Management System shall include support for Active Directory/LDAP to allow users to be added to the system. Use of Active Directory.LDAP requires that a server running Active Directory/LDAP , acting as a domain controller, to be available on the network.	
36	The Video Management System shall be designed to support each component on the same computer for efficiency in smaller systems, or each component on separate systems for large system deployments.	
B	Edge Storage	
1	Edge storage shall secure that when a lost or broken connection is back up, the data stored on the camera's internal storage shall be retrieved and stored in the media database. Edge storage shall secure that after recovery from a malfunction it shall be possible to play back and view the video, and audio recorded by the device, while the malfunction persisted	
C	Bookmarking	
1	A bookmarking feature shall be included in the Video Management System, allowing the client viewer users to mark incidents on live and/or playback video streams.	

D	Optimized Video Archiving	
1	Administrators shall be able to select a storage container for each device and move a device from one storage container to another, or move all recordings inclusive archives to the new storage container, or delete them all.	
2	Administrators shall be provided with an overview of the defined storage containers, their archives with path, and free and used space on the drives for each device, including the used storage space in the recording database, and in archives.	
E	Failover Support	
1	The system shall support automatic failover for recording servers. This functionality must be accomplished by a failover server that shall work as a standby unit, which takes over in the event that one of a group of designated recording servers fails. Recordings shall be synchronized back to the original recording server once it is back online.	
G	Multi-streaming Support	
1	The recording server must accept, display and record individual streams of video from each camera that supports it, for example, display a stream in H.264 format and record another stream in MPEG4 format. The intent of this functionality shall be providing independent streams of video from the camera to the server with different resolution, encoding and frame rate.	
2	Multi-streaming support shall allow the system to be configured with H.264 with a high frame rate for live viewing and shall allow the system to be configured with high resolution H.264 at low frame rates for recording and playback.	
3	The system shall allow recorded video to be recorded at 8fps.	
H	Alarms Support	
1	The alarm support shall allow for continuous monitoring of the operational status and event-triggered alarms from servers, cameras and other devices.	
2	The alarm support shall provide a real-time overview of alarm status, or technical problems, while allowing for immediate visual verification and troubleshooting.	
I	Matrix Functionality	
1	The system shall include an integrated matrix solution for distributing video to any computer with the client viewer installed. A computer on which the matrix-triggered images can be shown must be known as a matrix recipient.	
2	The client viewer shall provide remote users with a comprehensive suite of features:	
3	It shall be possible to playback recordings from cameras on the surveillance system, with a selection of advanced navigation tools, including an intuitive timeline browser.	
4	It shall be possible to access views of cameras on any PC with a client viewer application installed.	
5	It shall be possible to use multiple screens as well as floating windows for displaying different views simultaneously.	

6	It shall be possible to quickly substituting one, or more of a view's cameras with other cameras.	
7	It shall be possible to view video from selected cameras in greater magnification and/or higher quality in a designated hotspot.	
8	It shall be possible to receive and send video through the matrix functionality.	
9	It shall be possible to include HTML pages and static images (for example, maps, or photos) in views.	
10	It shall be possible to control PTZ cameras.	
11	It shall be possible to use digital zoom on live as well as recorded video.	
12	It shall be possible to activate manually triggered events.	
13	It shall be possible to activate external outputs (e. g. lights and sirens).	
14	It shall be possible to use sound notifications for attracting attention to detected motion.	
15	It shall be possible to get quick overview of sequences with detected motion.	
16	It shall be possible to get quick overviews of alerts.	
17	It shall be possible to quickly search selected areas of video recording for motion.	
18	It shall be possible to skip gaps during playback of recordings.	
19	It shall be possible to insert overlay buttons, for example, for activation of speakers, events, outputs, movement of cameras etc.	
20	It shall be possible to use a sequence function that lists thumbnail images representing recorded sequences from an individual camera or all cameras in a view.	
21	It shall be possible to use a forced playback mode allowing the user to playback recorded video from inside the 'live' mode while viewing 'live' video.	
22	The client viewer shall support the use of multimedia control devices, which are capable of emulating keystrokes, for the efficient review of recorded video.	
23	The client viewer shall support the use of keyboard shortcuts for control of standard features. It shall allow the user to program numerical keyboard shortcuts for camera views. The shortcut number shall be displayed with the view description in the live and playback displays. The shortcut shall allow the user to change views with 2 to 3 keyboard entries.	
24	The client viewer shall support GPU based video decoding to improve video rendering performance and up to 75% reduction in CPU load of the workstation running Client software. The use of GPU based video rendering shall also make client ready for 4K/UHD camera technology.	

25	The operator shall have the ability to use digital zoom where the zooming is performed in the image only on any number of cameras simultaneously. This functionality shall be the default for fixed cameras. The use of digital zoom shall have no effect on recording, or other users.	
J	Map Functions	
1	Built-in map function in the client viewer shall provide an intuitive overview of the system and shall offer integrated access to all system components.	
2	It shall be possible to use any number of layered maps, and it shall be possible to easily drag-and-drop and point-and-click definition of cameras, servers, microphones, speakers, I/O devices, hot-zones, and PTZ camera presets.	
3	Map function shall support instant camera preview when moving the mouse pointer over a specific camera.	
K	Remote Client Viewer	
1	The system shall support the use of separate networks, VLANs, or switches for connecting the cameras to the recording servers providing physical network separation from the clients,and facilitate the use of static IP addresses for the devices.	
2	The system shall support H.264, H.265 compression formats for all analog cameras connected to encoders, and all IP cameras connected to the system.	
3	The system shall support dual-streaming cameras and shall cover the following compression formats: H.264.	
4	The recording server shall utilize high performance ISCSI/SCSI/SAS and SSD disk	
5	The recording server(s) shall have the ability to support multiple Network Interface Cards (NIC) and shall support connection to the cameras on a network separate from the client viewer, management server and system manager.	
6	The recording server shall have the ability to accept the full frame rate supplied by the cameras, while recording a lower frame rate yet still shall make the higher frame rate available to the clients for live viewing.	
7	The VMS should be mandatory provided with number of Client Licenses as per the number of cameras mentioned in the SOR.	

33. Video Analytics- Technical Compliance

D.1.b	**Software for Video Analytics**		
S.No.	Type of Analytic	Specifications	Compliance
1	People Count	The analytic should have the capability of detection of a crowd within the Field of View of the camera and provide exact number of counts for the same.	

2	Intrusion	Intrusion VA Model should detect the presence of human within a defined polygon. Alert generation is controlled by the person count and the time period for which the person is present within the polygon	
3	Loitering	This feature should be enabled to detect human presence in a restricted zone for a time period greater than defined and raise an alert corresponding to the threshold breach,by maintaing continuous tracking of the person.	
4	Fence Climbing	This should help in detecting humans who climbs over a boundary wall or fence as defined using the ROI. IVA generates an alert when a person climbs or crosses over a wall or fence.	
5	Crowd Detection	The analytic should generate the crowd formation alert with estimate of the number of persons in the crowd based on the headcount, It should be possible for the operator to define the number of persons including within the crowd scenario.	
6	People Fight Detection	The objective of this usecase is to keep people safe and prevent accidents or criminal activities. Not all activities are easy to detect. For example, it is very difficult to detect if two people are fighting as this can take many different forms. However, many associated behaviors can be detected.	
7	Abandoned Object	The system shall be capable of detecting left objects that have remained stationary for a period of time that is considered suspicious by the user.The system shall have the ability to detect multiple objects that are left stationary in a scene.The user shall have the ability to configure the detection time to suit the environment.	

D.2	Software for Facial Recognition	
S no.	Description	Compliance
1	The FRS system shall have the best suited technology employed for 1:1 (one to one) and 1: N (one to many) matching application.	
2	The system shall have the provision to take multiple samples of same face belonging to same person.	
3	The system shall be able to add photographs obtained from law enforcement agencies to the criminals' repositories tagged for sex, age, scars, tattoos etc. for future searches.	
4	The system shall support diverse graphic formats.	
5	The system shall be able to check if new enrolled face is already enrolled in the data base before registering the new enrolled face in the system.	
6	The system shall have capacity to create different categories of people with option to customize the matching threshold for different categories.	
7	The system shall be able to utilize any of the file formats like JPEG, PNG, BMP, TIFF format for enrolment.	
8	The system for facial recognition or the forensic tool should be able to recognize partial faces with varying angles.	
9	The system shall be able to work on live full HD or Ultra HD Cameras.	

10	The system shall be able for matching suspect faces from pre-recorded video feeds obtained for CCTV deployed various identified locations.	
11	The system should be able to detect a face from a group photo.	
12	The system shall be able work on moderate face rotation either horizontal or vertical. It should support a yaw angle of -40 to +40 degrees, a pitch angle of -30 to +30 degrees and a roll angle of -30 to +30 degrees.	
13	The system shall be provided with watch list image database up to 100,000 for 1:N matching for live surveillance. The system should be scalable to upgrade to 250,000 for 1:N matching as and when required with additional license for watch list.	
14	The system shall be able to work on windows or Linux operating system.	
15	The system shall employ database system like MS SQL or Oracle or Postgre SQL or any other data base system.	
16	The image Database Server shall support redundancy with N:1 redundancy configuration.	
17	The system must perform a full 1:N search of the probe image in under 5 seconds against a database of up to 1 Million face records. The FRS should be considered to support 1 Million Face records.	
18	The system shall provide API to share the Facial recognition alert with VMS / ICCC application.	
19	The facial recognition system must support the ability the verify the quality of the enrolment image, including the following checks:	
a	Face reliability	
b	Eye distance	
c	Frontal score	
d	Face roll	
20	FRS Software vendor shall have mobile application of the same FRS software to support iOS and android based smart field devices. Mobile application shall be capturing the face of suspect in field and sending back to the FRS server for matching. Matching result shall be shown on the mobile application screen with matching score.	
21	The Face Recognition Algorithm should have participated and have been established in the Face Recognition Algorithm Evaluation conducted by NIST (National Institute of Standards and Technology, U.S. Department of Commerce) The NIST benchmark/ latest performance FRVT test results of current calendar year with respect to the opening date of tender or last 1 preceding year, the performance efficiency of the algorithm shall be within the top 25 ranked algorithms of the FRVT (1:N)results with FNIR (N=1.6M, T=0, Rank=1). test	

D.3	**Software for ICCC**		
S.No	**Component**	**Technical Compliances**	**Compliance**

1	Solution & Platform	The Command & Control solution should be implemented and complied to the industry open standards based Commercial-of- the-shelf (COTS) products.	
2		The Command & Control solution should be Micorservice based & support containerization of services.	
3		System must provide a comprehensive and industry accredited Unified Open Standard API (Application Program Interface) or SDK (Software Development's Kit) to allow interfacing and integration with existing systems, and future application and sensors which will be deployed on the field.	
4		System shall have capability to support future integration with department's future initiatives	
5		System should support Interoperability and Portability (replicable). System shall be able to integrate with any type of sensor platform or vertical solutions being used for the smart services irrespective of the technology used.	
6		Solution should not be dependent on properitory hardware.	
7		System shall be able to normalize the data coming from different devices of same type or different data sources and should suppport Common Standard Open Data Models for data normalization (i.e. Different VMS from different OEMs, etc.) and display unified view of alerts	
8	Command & Control Center Components	Web based application to provide access to alerts, event information, overall status, and dashboards.	
9		ICCC, through its integration with various smart devices and smart applications, will act as a Decision Support System for city administration to respond to the real time events by consuming data feeds from different data sources and by processing information out of these data sets	
10		Mobility: On field users should be able to view and update the incidents assigned to him / her.	
11		Security & Roles – should manage roles definition for internal as well as external access	
12		Centralized data storage for operational data : Should provide facility for centralized storage of operational data	
13	Incident Management	Should have an ability to display alarm condition through visual display and audible tone	
14		Should have an ability to simultaneously handle multiple alarms from multiple workstations	
15		Should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, severity, etc.	
16		Should display the highest priority alarm and associated data / video in the queue as default, regardless of the arrival sequence	
17		User should be able to change the priority of incident after providing valid comments	
18		Should support comprehensive reporting on event status in real time manually or automatically by a sensor, CCTV video feeds, any other sensor.	

19		Should support for sudden critical events and linkage to standard operating procedures automatically without human intervention. Operator should be able to associate pre-defined forms and attachments while handling an Incident in runtime.	
20		Should support for multiple incidents with both segregated and/or overlapping management and response teams.	
21		Should support Geospatial rendering of event and incident information.	
22		Should support incorporation of resource database for operation and mobilizing the field resources for response. Resources may be assigned and mobilized as per the defined Standard Operating Procedure in the system	
23	GIS Display	Shall have an ability to integrate with standard GIS maps.	
24		Shall view the environment through geospatial map and shall support OGC WMS standard.	
25		Shall allow user to view sensor and related name from the displayed map.	
26		Shall allow all resources, objects, sensors and elements on the map to be georeferenced such that they have a real world coordinate.	
27		Shall visually display a camera sensor and icons for different category of cameras.	
28		Shall visually display an alarming sensor on map.	
29		Shall visually differentiate sensor alarm on map through color and icon identifiers	
30	Video Display	Shall view live or recorded video from CCTV Camera / VMS	
31		Shall display video in 1x1, 2x2, 3x3 and 4x4 window formats	
32		Shall enable operator to specify video windows to be displayed in matrix	
33		Shall view either live or recorded video can be displayed in the video matrix window.	
34		Shall enable matrix settings to be saved per user	
35		Shall play, fast-forward, rewind, pause, and specify time to play recorded video	
36		Shall have the capability to move PTZ cameras	
37	Standard Operations Procedures (SOP)	Command & Control Center should provide for defininig un-limited number of configurable and customizable standard operating procedures through graphical, easy to use interface.	
38		Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.	
39		The users with administrative privilages should be able to edit the SOP, including adding, editing, or deleting the activities.	
40		In run time, users shall be able to modify tasks statuses on the list. They should be able to complete tasks, cancel them and mark them as ‘in progress’. Completing a task shall be as easy as checking a box after validating that all processes in SOP are completed.	
41		User should be able to see a graphical representation of SOP demarketing completed and pending tasks	
42		There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.	

43		The system will support post incident analysis through different reports generated that will enable the authorities to find gap/deficiency in the incident handling and help improve and/or rewrite SOPs	
44		The SOP Tool should have capability to define the following activity types:	
45		Manual Activity - An activity that is done manually by the owner and provide details in the description field.	
46		Automation Activity - An activity that initiates and tracks a particular work order and select a predefined work order from the list.	
47		If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.	
48		Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.	
49	Field Mobile User	The ICCC shall support mobile apps support for Android smartphones and tablets. The mobile apps shall communicate with the Mobile Server of the DC over any WiFi or mobile GPRS/3G/4G connection.	
50		Mobile User shall receive the alert from Operator to address the incident on field	
51		Mobile user shall provide function to update the status of alert, share input via message and close alert activities are completed	
52	Health Monitoring	Should provide icon based user interface on the GIS map to report non-functional device.	
53		Should also provide a single tabular view to list all devices along with their availability status in real time.	
54		The ICCC shall monitor the health of the system, log health related events, and calculate statistics like uptime, downtime.	
55	Dashboard & Key Performance Indicator	Real time dashboard on the situational view should provide information about security information so that officials have better understanding of what is happening on the ground.	
56		Command & Control Center should be able to facilitate measurement or criteria based on defined threshold values	
57		Green indicates that the status is acceptable, based on the parameters for that KPI, no action is required.	
58		Yellow indicates that caution or monitoring is required, action may be required.	
59		Red indicates that the status is critical and action is recommended.	
60	Reporting Requirement	The system should provide Informative and aesthetic dashboards providing simple clicks and friendly visualization	
61		User should be able to apply various predefined filters to the dashboard.	
62		The solution should generate reports of alerts/incidents based on the area, sensor type or periodic or any other customer reports as per choice of the administrators	
63	Authentication	Use authentication information to authenticate individuals and/or assign roles.	

64		Support LDAP authentication mechanism.	
65	Authorization & Access Control	Comprehensive policy-based security administration to provide all users specific access based on user's responsibilities for relevant web components. Maintenance of authorization policy in a central repository for administration purposes.	
66		Should support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure administration tools to manage users, groups, permissions and policies.	
67	Multi Level Access Control & Management	User will be defined with Geogrpaphy boundary to load the relevant sensors and alerts	
68		Escalation of alerts to next level if not addressed in defined time limit	
69		Central monitoring will have complete visibility of alerts and provide guidance to field operation team	
70	Administration Activities	The Configuration UI application shall allow the administrator or users with appropriate privileges to change the system configuration.	
71		The Configuration UI shall have a home page with single-click access to various tasks.	
72		The Integrated UI shall provide links to facilitate the following functions: • Configure Site hierarchy (multi level support expected) • Configure the Sensor systems (like VMS, FRS, PAS, ...) • Configure Users, Roles and Permissions • Configure Alert & related categories • Configure business rules and escalation rule	

D.4	Visitor Management Solution	
S.No	Parameter	Compliance
1	Enterprise Visitor Management Web based application with front end as ASP.NET and backend as MS SQL with admin, host employee and security gate module. The application should support upto unlimited employees database and visitors records.	
2	It should be Customizable as per the requirement, centralized, flexible and expandable architecture. The application can be integrated with 3rd party ACS seamlessly.	
3	Pre-Registration Page for the Visitors to directly assess the Registration Page & send request to the respective Host Employee request for a visit schedule.	
4	It should be integrated with SMS gateway and email interface	
5	Admin should have right to block the visitor and can put under watch list. Application should have fascility to scan visitor documents like Adhaar card, Photo ID card etc.	
6	Application should have facility to show visit list details:	
a	Waiting	
b	Visited	
c	Inside	

d	Denied	
7	It should have variety of reporting features as per the client requirement.	
8	System supports custom gate pass design : User should be able to define multiple gate gatepass profile	
9	Application has facility for sending SMS	
10	Application should have facility to import bulk employee data.	
11	User should be able to select the visitor &	
12	User should be able to Print the visitor pass	

D.5	EMS Application	
S.No	Parameter	Compliance
1	Fault & Perfromance Management	
2	Network Management	
3	Event Management	
4	Server, Storage and other Infrastructure Management	
5	Helpdesk Management And Reporting	
6	Asset Management	
7	SLA Management & Monitoring	
8	The proposed solution shall facilitate the analysis and display of status information from all network devices attached to the system that are SNMP and/or ICMP capable	
9	The proposed solution shall provide the ability to view the network and its associated IP SNMP/ICMP enabled devices including switches and other IP devices connected over the network.	
10	The proposed solution shall process atleast 2000 events/sec	
11	The proposed solution should include all hardware and software required to configure, control and monitor the network connected SNMP/ICMP based devices	
12	The proposed solution shall provide discovery & inventory of physical network devices and other IP devices	
13	The proposed solution shall be able to monitor the utilization of physical as well as virtual servers	
14	The proposed system shall employ Graphical User Interface that allows users to manage the network through a multilevel window. (i.e. Network and Sub networks Maps window)	
15	The help desk shall be a web enabled management system with SMS and email based alert system for the Helpdesk Call management and SLA reporting.	
16	Help desk facility shall be provided through Toll-free lines, landlines, helpdesk tool, E-mail, direct walk- in etc.	
17	Help desk shall track each incident / call to resolution. Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix agreed upon with Authority/authorized entity.	
18	Help desk shall analyze the incident / call statistics and provide monthly reports.	
19	Solution should also support Multitenancy	
20	Solution should support API integration with third party application	

21	Solution should have proper business intelligence tool	
22	Solution should cover all the aspects of FCAPS	
23	Solution Should support Automation from day one: Events should generates automatic tickets , automatically notfiy to field engineer regarding outages	
24	Solution shpuld support cloud and Virtualisation from day one	
25	Solution should support docker from day one	
26	Solution should support automatic incident notification to the field engg. via voice/sms from day one	
27	Solution should have predictive analysis from day one	
28	EMS /NMS /HELPDESK/ SLA MANAGEMENT & REPORTING should be from same OEM	
29	EMS shall support client–server based architecture. Client being GUI/web browser based access with secure interface to the server	
30	The EMS should support provision of creation, addition, deletion, updation and viewing capability of the managed network	
31	The EMS should support RADIUS based access control	
32	The proposed solution shall be capable of managing any SNMP/ICMP device from any vendor.	
33	Solution should have business serivce monitoring capabilty	
34	Solution shoud have role & privilages based access from day one	
35	Solution should support LDAP integration from day one	
36	Solution should support SSO from day one	

D.7	Single Sign ON (SSO) Application	
S.No	Description	Compliance
1	Solution should support authentication scheme that allows a user to log in with a single ID	
2	Following protocols should be supported for SSO: 1. SAML 2.0 2. oAuth 3. OIDC	
3	Solution should support self serivce portal for login into the integrated application	
4	Solution should be able to integrate with any third party applications or standards applications	
5	Should should support user & groups management	
6	Solution should support REST API based integration with third party application for the SSO	
7	Solution should be capable to do SSO for the legacy application as well	
8	Solution should support flexible RBAC model	
9	Solution should support flexible ABAC (Attribute access Control) model	
10	Solution should provide the ability to make real-time course-grained authorizationdecisions such as a whether to grant access to an application	
11	Solution should allow access and authorization permission criteria to be linked to roledefinitions rather than to individual user accounts so that these decisions are drivenby a user's membership of a role	
12	Solution should support nested roles and the dynamic assignment of roles (based onuser attributes	

13	Solution should provide a mechanism to authorize users based on data sourcesoutside the main solution identity data repository	
14	Solution should provide the configurable ability to restrict or allow concurrent loginsby the same user	
15	Solution should support time based access controls (e.g. acquiring temporary access rights for admin)	
16	Solution should support disablement/deletion of unused or expired accounts	
17	Solution should have user lifecycle management facility	
18	Solution should give the option for the newly logged in user to change his password and the user shall be forced to change the password first time	
19	Solution should provide option to authenticated user to change password.	
20	Password should be stored in encrypted format not in clear text	
21	Solution shall provide Password expiry date and can also be set/modified as number of days after which the user status will be changed as "Password Expired". By default the password expiry is enabled and set for specified day.	
22	Solution should be able to detect the failed login attempt for some specified number like 5, 10 times	
23	Solution should support auto generation password	
24	Solution should have ability to define the challenge response for the forgot password	
25	Solution should support self service portal for the reset password	
26	Solution should support encrypted password mechanism	
27	Solution should support strong password technicques for the powerfull login mechanism	
28	Solution shall support users belonging to multiple groups.	
29	Solution should be able to connect to variuos applications with independent databases so as to include all user profiles from those applications	
30	Solution should have the configurable ability to synchronize user account data with other authoritative data sources or repositories	
31	Solution should generate a unique user ID – a unique and permanent identifier to unambiguously identify every user in the solution identity data repository.	
32	Solution should be capable of identifying individuals who have more than one useraccount in the solution identity data repository, and merging these accounts into one	
33	Solution should support Event Based Logging	

D.8	Smart Class room solution		
S.No.	Component	Technical Specifications	Compliance
1	Interactive Flat Panel 75 inch	Panel Size: 75" or Higher	
		Type/Tech: IPS Type	
		Display Area (mm): Minimum 1649.644(H) x 927.936(V)	
		Aspect Ratio: 16:9	
		Native Resolution: 4K60hz	
		Colours: 10 bits	

		Brightness: Minimum 400 Nits or Higher	
		Contrast Ratio: 5000:1 (DCR)	
		Response Time: 8ms or Better	
		Viewing Angles: H = 178, V = 178 typ.	
		Backlight Life: Minimum 50,000hr of Higher	
		Surface Treatment: Hardness: 9H	
		Thickness: 4mm	
		Orientation: Landscape	
		Processor: Quad Core ARM Cortex-A73*4 or Higher	
		RAM: 4GB DDR4 or More	
		Storage: 32GB or More	
		Type/ Tech: IR Recognition/ P-Cap	
		Touch Point: 33 points or Higher	
		HDMI In: x3 (Front*1, Rear*2)	
		RGB / VGA: 1	
		DisplayPort: DP1.2*1	
		Audio In: PC audio in (3.5 mm)*1	
		RS232: x1	
		OPS: 1	
		Audio Out: 3.5mm x1	
		SPDIF: x1	
		RJ45: x1	
		Type A: USB 2.0 x1(Side x1)USB 3.0 x4 (Front x2, Side x2, port USB)	
		Type B: x2, for touch	
		In Built 8 Array Microphones	
		Type C: x1 (USB3.0, 60W PD)	
		SPEAKERS: 15W x 2 + 15W x 1	
		Power Consumption: 160W or Less	
		EEI rating certificate	
		Software Features	
		Entity Management & Device Manager to Manage IFP remotely without LAN, also to share Content & Broadcast Messages Remotely onto IFPs. Same Whiteboard Software for Windows, Android & Browser Live webcast directly from Interactive Whiteboard Software to YouTube and Facebook, Screen Recording	
		Artificial Intelligence Pen	
		Wireless Casting on IFP from Mobile & Laptop	
		Drag and Drop YouTube videos, Direct images from google search	
		Handwriting Recognition	
		Text to Speech inbuilt in Whiteboard Software (Male or Female Voice)	
		Create Online Quiz with Time Limit from Whiteboard Software	
		Auto Grading of answers	

		Download results as Excel sheets	
		Sign in directly from QR Code on Interactive Whiteboard Software and link	
		Cloud Storages (Google Drive, Microsoft One Drive, Box or Drop Box)	
2	Computing Device	Processor : Available in Intel i5/i7 Processor or AMD Ryzen 5/7	
		Memory Size : Support 32GB DDR4 RAM	
		Storage Slot : 1 x 2.5 HDD {Upto 2 TB) and 1 x MSATA {Upto 512 GB)	
		Wifi Connectivity : 802.11 b/g/n Dual Band 2.4/5.0 GHz	
		Ethernet : 10/100/1000 Mbps	
		Graphic : Intel Graphics 640 or equivalent	
		1/0 Ports : 6x USB 3.0 2 x USB 2.0 1x VGA 1 x HDMI 1 X RJ45 1 x HDD SATA Port {Supports 2.5" SATA & SSD) 1 x 3.5mm Audio Jack	
		1 x 3.5mm Mic. Jack	
		1 x Power Button	
		1 x DC in "	
		Fan : Built in non-noise Fan	
		Environment : 0°C ~ 40°C { 32°F ~ 104°F) at 0.7m/s Air Flow	
		Relative Humidity : 75% @ 35°C {non-condensing)	
		Material: Aluminum Alloy	
		Device Size: 20*18*4cm {LxWxH)	
		Device Weight: 984g	
		Power: 12V/5A	
		Supported Operating System: Windows 7/8/10/11	
		(Pro/Home/lOT/Ulimate), Ubuntu/LINUX/CENTOS/LEDS/ESXI 6.7 etc.	
		Mouse: 2 Button USB optical Scroll mouse	
		Keyboard: 104 keys multimedia USB Keyboard with ₹ symbol	
3	Facial Recognition based Attendance Solution	Web-based- Deployment of Student Database Management Information System (SDMIS) which captures the complete details of Student and staff to mark attendance.	
		AI enabled – Deployment of Artificial Intelligence based Solution to register, identify and capture the attendance of the students and staff. MIS Reports - Solution should have a report engine to generate attendance reports	

D.9.a	Boom Barrier	
S.No	Parameter	Compliance

1	Size	3 meter to 6 meter & up to scalable with custom design	
2	Type	Semi-Automatic, Automatic	
3	Color	any	
4	Power	50/60Hz	
5	Max Power	240 W	
6	Voltage	110V/220V +/- 10%	
7	Material	Stainless Steel, Aluminium, Iron	
8	Weight (Kg)	40 to 80 Kg	
9	Opening Time	2 to 5 sec	
10	Power Source	Electric	
11	Operative Options	Remote Control & amp; Push Button	
12	Working Temperature	-20 degree to 60 degree C	

D.9.b	Baggage Scanner		
Sr. No.	Technical Description		Compliance
A. General Specification:			
1	Tunnel Opening:	600 mm x 400 mm (+/- 2%)	
2	Power Requirements:	220VAC:183-253 VAC,50Hz, 6 Amp Max	
3	Color Imaging:	3 Colors imaging based on atomic number and 6 colors imaging based on atomic number.	
		Ability to move between 3 color and 6 color during baggage scanning in real time	
4	Video Display:	22'' high Resolution, Low Radiation, Ergonomic, LCD Color Monitor	
5	Power Consumption:	Should not exceed 0.5 KV on full load	
Image Processing:			
6	Penetration:	In Steel 35 mm Guaranteed	
7	Wire Resolution :	40 AWG Wire Typical, 38 AWG Guaranteed	
8	Contrast Sensitivity:	24 Visible Levels, 4096 Gray Levels	
9	Beam Divergence:	Beam Divergence : 74° diagonal Vertically up-word	
10	Display Resolution:	1920 x 1080; 24 bit/pixel color	
11	Material Discrimination:	Organic and inorganic material discrimination based on atomic number and density. 1 liter bottle of water should completely come in orange color shades only when put in multiple orientations (horizontal/vertical) in a bag	
12	Resolution and Penetration	Both resolution and penetration should be seen without press of a button with free style	
X-Ray Generator:			
13	Voltage:	160 KV	
14	Tube Current:	0.7 mA	
15	Cooling:	Sealed Oil Bath	
16	Duty Cycle:	100%	
17	X-Ray Detector:	"L"-Shaped array	

Environmental Condition:			
18	Storage Temperature:	-20^{o}C to 55^{o}C (Govt Lab test report to be enclosed)	
19	Operating Temperature:	0^{o}C to 55^{o}C (Govt Lab test report to be enclosed)	
20	Humidity:	Up to 95% non-condensing	
Physical Specification:			
21	Dimensions:	1800 mm(L) x 900 mm(W) x 1330 mm(H) approx	
22	Conveyor Belt Height:	Range of 750 mm and adjustable 100 mm	
23	Conveyor Speed:	0.18 to 0.2 m/s in forward & Backward direction	
24	Conveyor load:	Mim160 kg evenly distributed	
25	Input / Output roller tables	Should be 500 mm each	
26	The vendor shall supply rodent protection, anti-rodent and dust prof cover		
27	Inbuilt type Control desk with security housing and locking provision should be available		
28	Machine should be Indigenous make		
Computer Specification:			
29	At a minimum:		
	1. OS: Should be Windows based-Windows 10 prof minimum		
	2. Processors:- Minimum Core i5, 3.0 GHz processer ,		
	3. Memory:- Minimum 8 GB Ram,		
	4. Storage Capacity:- Minimum 1 TB HDD/SSD,		
	5. Video card:- 2 GB GU		
	6. UPS:- UPS for entire machine with power backup time of 15 minutes for the machine load.		
Software Feature:			
30	All software features of machine should be online and password protected		
31	Advanced Image Archive, up to 200,000 images		
32	All image processing should be possible from monitor via mouse and also from keyboard		
33	System should have PAN Option		
34	Date and Time Display		
35	Inverse/Negative black and white Imaging		
36	Inverse/Negative color imagining based on atomic number		
37	High Density Alert - Audio visual alarm and draw square around the object area where High density is found		
38	Baggage Counter		
39	Horizontal and Vertical Imaging		
40	Print Image Function if printer is connected		
41	Successful logging in and logging off to be displayed		
42	Pseudo color and reverse Monochrome		
43	4 Level of access		
44	2X to 64X Zoom		
45	User Defined manual and automatic Access to Image archive		
46	Programmable Penetration and Contrast levels		
47	Organic and Inorganic Imaging		
48	Color and Black & White Imaging		
49	Edge-enhancement Imaging		

50	Machine should be capable of recalling 15 previous images	
51	Organic & Inorganic material discrimination	
52	The system should be user friendly	
53	TIP should be available and programmable and ability to automatically lock user if configurable “Miss” attempts exceeded.	
54	Variable brightness	
55	Auto Centering of Images	
56	High Low Penetration - Clearly show metal objects below 35 mm of steel	
57	Display language for user interface should be English and Hindi (for easy understanding)	
Health and Safety:		
58	Film Safety : Guaranteed up to ISO 1600 (33 DIN)	
59	Maximum leakage radiation less than 0.1 mR/hr(1µ Sv/hr)	
60	The system should have three Emergency stops switches, X-Ray on Indicator, Supply on Indicator, Programmable audio-visual alarm	
61	AERB certificates likes manufacturing license, type test approval certificate should be uploaded with tender	
62	The systems should be food safe and AERB/BARC certificate enclosed with tender.	
63	Suitable lead impregnated rubber curtains at both ends of tunnels	

D.10	ANPR Solution	
S.No	Description	Compliance
1	ANPR Platform shall be on microservice based architecture and support the configuration/management of the following components specific to ANPR: • ALPR units and cameras. • Hotlists and Wanted vehicles • It shall be possible to view video associated to ALPR events when viewing a report. • Pattern of vehicle number plates if found new to be incorporated and given to OCR additions.	

D.11	IPBX Solution	
S.No	Parameter	Compliance
1	EPABX with Voice Gateways/server to connect Hybrid phone extensions & Trunk lines.	
2	Operator console :1 no’	
3	IP phone TYPE-1 required with system upto 700 nos	
4	IP phone TYPE-2 required with system upto 400 nos	
5	Analog Phone upto 400 nos.	
6	Server based Hybrid PBX systems for multilocations	
7	should be configured with Analog extension ports 350, IP extension licenses & Phones 1000, 2 PRI,10 Analog trunk line ports,	
8	Hard and PC based operator console 1 with extra button module. With features like High availability, call control, mobility, centralized license,	

	multiparty audio conference, voice mail and auto-attendant. Gateway & Redundant server	
9	IP based Unified Communications Solution designed for requirements, supporting up to 5,000 users at a single location in future with additional components. For businesses with multiple locations, streamline operations, centralize management,	
10	Can be configured as a voice-only PBX using traditional circuit-switched lines or as an IP telephony server using high-speed ISDN/PRI dial-up access And/or direct leased line connectivity and/or SIP trunks.	
11	including Analog, IP/SIP Desk phones, Conference Phones and also the next generation PC based and Android/iPhone/iPad based Mobile Softphones	
12	System Has facility to connect Hybrid extensions (Analog, digital and IP based extensions)	
13	The system should be expandable to 5,000 extensions (any combination of Digital/ Analog/IP/DECT)	
14	The offered system should be hot standby configuration with transparent switchover on occurrence of fault, from the main to the standby set. The same should also be duplicated to support Hot Swap-ability of Control Cards & Power Supply and the ongoing call (Analog, Digital Phones & IP Phones) should not be disconnected during the changeover or physical removal of either of the set, programmed as Active.	
15	Server should Use of Solid Stage Drive (SSD) for more reliability of database, HDD based solution will not be accepted.	
16	SSD for database storage,Two SSD slots thereby offering SoftRAID-1 reliability	
17	The Server should have a redundant power supply and should support AC / DC power supplies providing redundancy.	
18	Server should have redundant DC Power supply for automatic switchover for redundancy	
19	The offered system should be a standard 19’inch rack-mountable solution / Server based	
20	The preferred server operating system is Linux	
21	Complete system back up including OS (ISO image) can be kept on simple USB drive.	
22	The Server should be ENERGY STAR certified	
23	The memory shall be based on Solid state Drive technology for higher reliability and faster rebooting.	
24	All the peripheral cards (Extension card, Trunk Card, ISDN Card, etc) shall be Hot Swappable, i.e.; It shall be possible to replace a peripheral card while the power is on.	
25	The offered server should support IP Remote stackable Gateway or standard 19" rack mountable Chassis based Gateway	
26	Gateway should have universal slot for Analog/Digital/IP interface cards, FXO & FXS based gateways are not acceptable	
27	IP Remote stackable Gateway should support (a) minimum 150 TDM extension and all features and applications of the central system, (b) administration of all components via central management tool, (c) integrated echo compensation, (d) voice compression according to ITU-T G.711 and G.729 AB	

28	All analogue trunks and analog extensions should have Caller ID for internal and external incoming calls.	
29	IP Phones should support voice codec G.711 (64 kbit/s a/µ-law), G.722 (64 kbit/s), G.729AB (8 kbit/s), OPUS, PoE (IEEE 802.3az) and have 10/100/1000 MBPS LAN ports.	

E.1	Video Wall		
S.No	Parameter	Specification	Compliance
1.	Display Wall Individual Cube Size	70 Inch with 2x3 configuration	
2.	Projection Technology	DLP Rear Projection with each cube having 4K-UHD resolution	
3.	Individual Video Wall Resolution	15360 x 8640	
4.	Cube Depth	Less than 600 mm	
5.	Light Source	Laser	
6.	Light Output of projection engine	2200 Lumens or more	
7.	Brightness Uniformity	95%	
8.	Dynamic Contrast ratio	100,000:1	
9.	Dust Proof	Projection Engine to be certified IP6X by a third-party laboratory to ensure prevention from ingress of dustw ensuring long life of the video wall	
10.	Power Supply	Dual Redundant Power Supply Built in inside the cubes	
11.	Half Gain viewing angle	Horizontal ± 36°, Vertical ± 34°	
12.	Lifetime	Normal mode: 60 000h	
		Eco mode: 90,000 Hours	
13.	Inputs	1 x Display Port 1.2, 1 x HDMI 2.0	
14.	Power	100 - 240 VAC, 60 - 50Hz, (below values are for 230V; 110V +5%)	
15.	Normal mode	Less than 350 Watt	
16.	Normal mode	Less Than 1200 BTU/h	
17.	Operating conditions	5 Degrees to 40 Degrees C	
18.	Humidity	Up to 80% non-condensing	
19.	Temperature	10°C-40°C | 50°F-105°F	
20.	Temperature	0°C-40°C | 32°F-105°F	
21.	Video Wall and cube Control	Management through IP and handheld Remote Control for quick access	
22.	Screen Backing	3-layer screen with hard backing	
23.	Screen to Screen Gap	0.2 mm or lower at temperatures between 20~25 deg C.	

E.2	Video Wall Controller		
S.No	Parameter	Specification	Compliance
1		As per standard OEM solution	

E.3	Audio Mixer and Speaker System		
S. No.	Parameter	Specification	Compliances
1	Audio Mixer	Input Power 6W RMS	
2	Frequency Response (-3dB)	80Hz - 18kHz or better	
3	Frequency Range (-10dB)	150Hz - 15kHz or better	
4	System Sensitivity (1W @1m)	89dB / 90.8 dB / 108.8 dB or better	
5	Nominal Impedance	16 Ohms	
6	Speaker Mounting	Ceiling Speaker	
7	SNR	>= 70 dB	
8	Speaker Output	100 V AB 6 Zone Speaker Output	
9	Operation Environment	Operation Temp: +5 °C ~ +40 °C	
		Store Temp: -20 °C ~ +70 °C	
		Operation Humidity: <95%	

E.4	Multi-Function Laser Printer		
S.No	Parameter	Specification	Compliance
1.	Resolution (black)	Up to 1200 x 1200 dpi or better	
2.	Resolution (color)	Up to 1200 x 1200 dpi or better	
3.	Paper trays, standard	3	
4.	Print technology	Laser	
5.	Display	4-line LCD (color graphics)	
6.	Number of print cartridges	4 (1 each black, cyan, magenta, yellow)	
7.	Connectivity	2 Hi-Speed USB 2.0 Host ports; 1 Hi-Speed USB 2.0 Device port; 1 Gigabit Ethernet 10/100/1000T network port; 1 Hardware Integration Pocket; 2 internal USB Host ports	
8.	Processor speed	Minimum 700 MHz or better	
9.	Paper handling input, standard	100-sheet multipurpose tray, 500-sheet input tray 2, 500-sheet heavy media input tray 3	
10.	Paper handling output, standard	250-sheet output bin	
11.	Duplex printing	Automatic (standard)	
12.	Hard disk	Standard, 250 GB minimum	
13.	Print speed, black (normal)	Up to 33 ppm	
14.	Memory	Minimum 512 or higher	

15.	Media sizes supported	Tray 1: A4, RA4, A5, B5 (JIS), B6 (JIS), 10 x 15 cm, A6, 16K, envelopes (B5, C5 ISO, C6, DL ISO); custom: 76 x 127 to 216 x 356 mm; Tray 2: A4, A5, B5 (JIS), B6 (JIS), 10 x 15 cm, A6, 16K; custom: 102 x 148.5 to 216 x 297 mm; Tray 3: A4, RA4, A5, B5 (JIS), 16K; custom: 148.5 x 216 to 210 x 356 mm	
16.	Compatible operating systems	Microsoft Windows 7 Professional(64bit), Windows 8 Pro (64 Bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux	

E.5	LED Television Set		
S.No	Parameter	Specification	Compliance
1.	Display Type	Ultra HD 4K	
2.	Screen Size (Diagonal)	138.8 cm (55 inch) minimum or more	
3.	Screen Resolution	Minimum - 3840 x 2160 - Ultra HD	
4.	HDMI & USB Ports	Minimum 2 USB Ports and 1 HDMI Ports	
5.	TV Connectivity	Built-in Chromecast and WiFi	
6.	Speaker Output Power	Minimum 2 X 10 Watts	

E.8	Air Conditioning		
S.No	Parameter	Specification	Compliance
1	Product Type	Split	
2	Capacity	2 Ton	
3	Energy Efficiency	5 Star	
4	Energy Efficiency (EER (Cooling, W/W))	3.4 or better	
5	Noise Level (Indoor, High/Low, dBA)	45 / 37 / 28 or better	
6	Noise Level (Outdoor, High/Low dBA)	54	
7	Power Source(Φ/V/Hz)	1/230/50	
8	Power Consumption (Cooling, W)	Avg. 2100 or less	
9	Operating Current (Cooling, A)	9.5 or better	
10	Piping Length (Max, m)	25 or better	
11	Piping Height (Max, m)	10 or better	
12	SVC Valve (Liquid (ODxL))	6.35	
13	SVC Valve (Gas (ODxL))	15.88	
14	Moisture Removal (l/hr)	2.5	
15	Air Circulation (Cooling, ㎥/min)	17.5 or better	
16	Refrigerant (Type)	R410A	
17	Low Ambient (Cooling, ℃)	16 ~ 52	
18	Outdoor Unit (Compressor Type)	BLDC	
19	Outdoor Unit (Anti-Corrosion Fin)	Yes	
20	Outdoor Unit (Multi-Channel Condenser)	Yes	
21	Air Direction Control (Up/Down)	Auto	

E.9	150 KVA UPS		
S.No	Parameter	Specification	Compliance
1.	Capacity	150 KVA with N+1 Redundancy	
2.	Technology	IGBT (Rectifier & Inverter both); ECO Mode required with Inbuilt Isolation Transformer	
3.	Wave form & Freq converter	Pure Sine wave & shall have frequency converter mode	
4.	Display	LCD	
5.	Input power factor correction	0.99 at 100% Linear load	
6.	Input configuration	3Ph, L-N+PE, +/- 10% on full load	
7.		UPS Shall have inbuilt Input Isolation Transformer	
8.	Frequency (Input)	45 to 55 Hz frequency (or 54 to 66 Hz for 60Hz Output)	
9.	Frequency (output)	50Hz or (selectable to 60Hz)	
10.	Output Voltage	220/230/240Vac shall be available with +/-1% regulation	
11.	Output Voltage Distortion	< = 3% max full linear load	
12.	Output Power factor	0.9	
13.	Crest factor	3 or better	
14.	AC-AC Efficiency	Online Mode: Greater than or equal to 88% @ Full Rated Load & Battery Fully charged	
15.	Transfer time Main-Battery	0	
16.	Transfer time Inverter-Bypass	4 msec	
17.	Output Connection	Hardwired Terminal Block required	
18.	Monitoring software for UPS	Shall be provided for monitoring of UPS from remote along with SNMP Card, this project being of high security & safety the SNMP card.	
19.	Communication	SNMP	
20.	Port	RS 232	
21.	Battery Type	12V SMF.	
22.	Battery backup	150KVA UPS with 30 min battery backup at 80% load (9984 VAH or more)	

23.	Charger	Shall be minimum 10% of the offered Battery AH	
24.	Battery Flexibility	32 to 40 Battery Flexibility required	
25.	Environmental Parameter		
A	Operating temperature range	0-40 deg C	
B	Other	Indication required -> Over Temperature, Load on Battery, Battery low, Mains ON	
C	Humidity	5% to 95% no-condensing	

E.10	Electrical and power cabling		
S.No	Parameter	Specification	Compliance
1		Standard as per solution requirement	

E.11.1	Water Leakage Detection System	
S.No	Parameter	Compliance
1	The Water leak detection system should comprise of Sensor rope, Water Leak detection modules, I/O modules and sounders all connected to a Control Panel.	
2	It should consist of leak detection cable and an alarm module.	
3	The cable should be installed in the floor areas around the periphery of DR Data Center.	
4	Water Leak Detection sensors should be able to mount in DIN rails, inside AHU's, power distribution units or other equipment where localized leak detection is required.	
5	The detectors should be resistant to oxidation and erosion.	
6	The detector should have relay output forconnection to the controller.	
7	LED alarm as well as audio alram indication should also be provided.	
8	The detectors should operate in AC or DC supply.	

E.11.2	Rodent Repellent System	
S.No	Parameter	Compliance
1	The Data Centre and UPS & Electrical Room should be protected with Ultrasonic Rodent Repellent System.	
2	Operating Frequency : Above 20 KHZ and below 60 Khz or better	
3	Sound output : 80db to 110db at 1metre or better	
4	Power output : 1W per transducer	
5	Sweeps per Minute : 130(Configurable)	
6	Frequency Division : 100(Configurable)	
7	Power Consumption : 15 Watts Approximately	
8	Power Supply : 230V AC/ 50Hz 14 Volts DC	

9	Dimensions : 270(W) x 100(H) x 320(D)mm or any	
10	Weight : 6.5 Kgs Approx or any	
11	Mounting : Wall / Table Mounting	

E.12	LAN and CAT-6 cabling	
S. No.	Description	Compliance
1	Standard as per solution requirement	

E.13	Fire & Smoke Detection System	
S. No.	Description	Compliance
1	Standard as per solution requirement	

E.14	Control Room Operator Desks	
S. No.	Description	Compliance
1	Standard as per solution requirement	

E.15	Conference Room for internal meeting	
S. No.	Description	Compliance
1	Standard as per solution requirement	

E.16	Interior work with furniture for operator workstation, executive chairs, desk.	
S. No.	Description	Compliance
1	Standard as per solution requirement	

F.1	144 Core Multitube Single mode	
S. No.	Description	Compliance
1.1	Shall be Single mode (OS2), FRLSZH Single Jacket, Single Armor, Gel-free, Fiber Cable.	
1.2	Applicable Qualification Standards shall be EN 187105, EN 50173 and Telcordia GR-20 & GR-409. Standards Compliance: ITU-T G.652.D, ITU-T G.657.A1 (Bend insensitive) and ANSI/TIA-568 C.3 (OS2).	
1.3	RoHS 2002/95/EC compliant.	
1.4	Total number of fibers shall be 144, with 12 loose tubes (Gel Free), each having 12 fibers.	
1.5	The Fiber shall have HDPE/MDPE outer jacket, with Corrugated Steel Tape Armoring with FRLSZH Sheath as per IEC 60332-3.	

	The Fiber shall be Black in color to ensure UV stabilized. The Fiber shall have Water Swellable Tape & Water Swellable Yarns to protect the fiber cores from water.	
1.6	Maximum Cable Diameter shall be 16 ± 5 % with a Cable Weight of 155 kg/km ± 10%.	
1.7	The Tensile Load should be from 2200 N to 2700 N. Central strength member shall be FRP Rod.	
1.8	The Fiber shall be suitable for Aerial (lashed), Indoor and Outdoor Ducts or Direct Burial applications. The Installation Temperature shall be -20 degree Celsius to +70 degree Celsius, Operating Temperature shall be -20 degree Celsius to +70 degree Celsius.	
1.9	The maximum attenuation shall be 0.22 dB/km @ 1550 nm, 0.31 dB/km @ 1380 - 1386 nm and 0.34 dB/km @ 1310 nm. The Chromatic Dispersion @ 1310 nm ps/nm x km ≤ 3.5 & @ 1550 nm ps/nm x km ≤ 18 The maximum cabled cutoff wavelength shall be 1260 nm.	

F.2	144 LC Fiber port Single Mode OS2 intelligent loaded LIU	
S. No.	**Description**	**Compliance**
5.1	Shall accommodate 8 Adapter plates or 8 pigtail cassettes for a total of 144 fiber terminations.	
5.2	The width shall be 19 inches and height of 2U (3.5 inches), with a maximum of 20-inch depth.	
5.3	The shelf/LIU shall be sliding, and LIU material should be steel.	
5.4	The Fiber shelf must be Intelligent ready and must support field upgrade to intelligent fiber panels without removal of existing patch cords and without disruption of network services.	
5.5	Shall have splice trays to splice minimum 144 fibers.	

F.3	Joint encloser	
S. No.	**Description**	**Compliance**
4.1	Shall be a butt type enclosure with a dome and base (IP 68 Rated)	
4.2	The Cable entries should be through the cable ports located in the base.	
4.3	The dome and base should be sealed using a clamp with O-ring system. The cable entry ports should be sealed mechanically instead of heat shrink.	
4.4	This block can be opened and closed repeatedly without the need to remove or replace the gel.	
4.5	General Specifications	
	a) IP68 Rated	
	b) No. of Splice trays: 6 nos.	
	c) Splice Tray Capacity: 24 Fibers	
	d) No. of cable entry ports: 4 round ports and 1 oval port.	
4.6	The closure should have the capability to accommodate loop cables (uncut loose tube cables)	

4.7	The cables should be secured to the closure using hose clamps and a cable attachment device.	
4.8	The closure should have a basket for storing loose tubes.	

F.4	Outdoor Street cabinet IP 55 rated	
S. No.	Description	Compliance
9.1	**Street Cabinet/Fiber Distribution Cabinet** the Street cabinet shall be used for Fiber Cable distribution at field side and is a plinth mountable outdoor unit, **IP 55 Rated**. It should at least have the following features:	
	a) Should be loaded with adequate number of SCAPC Adapters and pigtails so that all the Distribution fiber ports can be patched to the incoming and outgoing main cables. The numbers of Ports shall exceed 12 numbers at the maximum.	
	b) Should have provision for loading up to 4 nos. of 24F splice trays, the product should be loaded with adequate number of splice trays for splicing the conventional fibers.	
	c) The splice trays should be Round splice trays with individual slots in the fiber distribution cabinet.	
	d) The tray fitment should be available at the rear wall of cabinet with individual slots for easy access.	
	e) The splice tray holder should be available at the center of the circular tray for 24F.	
	f) The box should have the provision to terminate 10 nos. Armoured drop cable and 1 no. of 12 Fiber cable.	
	The adapter panel should have the following features	
	i. The panel should be swing out type for easy access.	
	ii. The 12F, Main Fiber Cable & Distribution fiber Cable inputs and outputs should be patched to the front of the adapter panel	
	iii. The Panel should have Fiber Splitter slots, minimum 4 Nos.	
	iv. The pigtails should be patched to the rear of the adapter panel.	
	v. The adapter panel should be pre-loaded with adequate number of SCAPC adapters and pigtails so that all the splitter ports can be patched to the incoming and outgoing main and distribution cables.	
	vi. The cabinet should have the parking lot available for splitters unused ports.	
	vii. There should be a provision for fixing **96F** simplex adapters.	
	viii. The adapters should be fixed using screws to the adapter panel.	
	ix. Should be loaded with adequate number of splice trays for splicing the GPON as well as the conventional fibers.	
	x. The blank adapter ports should be closed with plastic blanking plugs	
	a) Basket should be provided for looping the uncut loose tubes	
	b) The Cabinet should have locking System.	
	c) The cabinet should have document holder.	
	d) The Cabinet should have plinth for easy cable entry	
	The cabinet should be supplied with all the required accessories for installation viz. Fusion splice protectors (40mm), cable ties, IPA, tissue paper, hose clamps, red adhesive tape, grounding accessories, route card, transport tube (non kinking type 3mm diameter), cable ties, foam tape.	

F.5	Fibre Patch Cord- SCAPC SCAPC, Single Mode Fiber Patch Cord, Simplex.	
S. No.	Description	Compliance
10.1	**Make and Type** Shall be Single mode (OS2), SC APC to SC APC, Simplex Fiber patch cords.	
10.2	Standards Compliance: G.652.D, G.657.A1 and OS2	
	Regulatory Compliance: RoHS 2011/65/EU	
	Cable Qualification Standards: ANSI/ICEA S-83-596 and Telcordia GR-409. Optical Components Standard: ANSI/TIA-568-C.3	
10.3	**General Specifications**	
	Connector Color: Green	
	Connector Interface: SC APC & SC APC	
	Operating Temperature: -10 degree Celsius to +60 degree Celsius	
	Length Shall be 1/2/3/5/10 meters	
10'.4	Connector Optical Performance	
	Insertion Loss, Typical: 0.30 dB	
	Return Loss, minimum: 65.0 dB	
10.5	**Temperature Range:** -10 Deg. C +60 Deg. C	

F.6	12 Core Single Mode	
S. No.	Description	Compliance
2.1	Shall be Single mode (OS2), FRLSZH Single Jacket, Single Armor, Gel-free, Fiber Cable.	
2.2	Applicable Qualification Standards shall be EN 187105, EN 50173 and Telcordia GR-20 & GR-409.	
	Standards Compliance: ITU-T G.652.D, ITU-T G.657.A1 (bend insensitive) and ANSI/TIA-568 C.3 (OS2).	
2.3	RoHS 2002/95/EC compliant	
2.4	Total number of fibers shall be 12, with 2 loose tubes (Gel Free), each having 6 fibers.	
2.5	The Fiber shall have HDPE/MDPE outer jacket, with Corrugated Steel Tape Armoring with FRLSZH Sheath as per IEC 60332-3.	
	The Fiber shall be Black in color to ensure UV stabilized.	
	The Fiber shall have Water Swellable Tape & Water Swellable Yarns to protect the fiber cores from water.	
2.6	Maximum Cable Diameter shall be 13 ± 5 % with a Cable Weight of 150 kg/km ± 10%.	
2.7	The Tensile Load should be from 2200 N to 2700 N.	
	Central strength member shall be FRP Rod.	
2.8	The Fiber shall be suitable for Aerial (lashed), Indoor and Outdoor Ducts or Direct Burial applications.	
	The Installation Temperature shall be -20 degree Celsius to +70 degree Celsius, Operating Temperature shall be -20 degree Celsius to +70 degree Celsius.	

2.9	The maximum attenuation shall be 0.22 dB/km @ 1550 nm, 0.31 dB/km @ 1380 - 1386 nm and 0.34 dB/km @ 1310 nm.	
	The Chromatic Dispersion @ 1310 nm ps/nm x km $\leq$ 3.5 & @ 1550 nm ps/nm x km $\leq$ 18	
	The maximum cabled cutoff wavelength shall be 1260 nm.	

F.7	24 port LC Single Mode OS2 intelligent loaded LIU	
S. No.	Description	Compliance
6.1	Shall accommodate 4 coupler plates or 4 pigtail cassettes for a total of 48 fiber terminations.	
6.2	The width shall be 19 inches and height of 1U (1.75 inches), with a maximum of 20-inch depth.	
6.3	The shelf/LIU shall be sliding, and LIU material should be steel.	
6.4	The Fiber shelf must be intelligent ready and must support field upgrade to intelligent fiber panels without removal of existing patch cords and without disruption of network services.	
6.5	Shall have splice trays to splice minimum 32 fibers.	
6.6	Each module shall accommodate 12/24 fibers, with 12/24 LC adapters.	
6.7	The adapter module shall be intelligent upgradable without any interruption to service due to patch cord removal or through re-splicing. The module should only accept standard patch cords and no 9th pin, RFID, CPID etc. will be accepted.	
6.8	The adapter color shall be blue for Single mode.	

F.8	Fibre Patch Cord- LC-LC Single Mode	
S. No.	Description	Compliance
8.1	Shall be Single mode (OS2), LC to LC, Fiber patch cords.	
8.2	Standards Compliance: G.652.D, G.657.A1 and OS2	
	Regulatory Compliance: RoHS 2011/65/EU	
	Jacket: Low Smoke Zero Halogen (LSZH) compliant to IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE 383, UL 1666, UL 1685	
	Flame Test Listing: NEC OFNR-LS (ETL) and c(ETL)	
	Cable Qualification Standards: ANSI/ICEA S-83-596 and Telcordia GR-409	
	Optical Components Standard: ANSI/TIA-568-C.3	
8.3	General Specifications	
	Connector Color: Blue	
	Connector Interface: LC	
	Operating Temperature: -10 degree Celsius to +60 degree Celsius	
8.4	Connector Optical Performance	
	Insertion Loss, Typical: 0.20 dB	
	Return Loss, minimum: 55.0 dB	

F.9	06 Core, Single mode	
S. No.	Description	Compliance
3.1	Shall be Single mode (OS2), FRLSZH Single Jacket, Single Armor, Gel-free, Fiber Cable.	

3.2	Applicable Qualification Standards shall be EN 187105, EN 50173 and Telcordia GR-20 & GR-409.	
	Standards Compliance: ITU-T G.652.D, ITU-T G.657.A1 (bend insensitive) and ANSI/TIA-568 C.3 (OS2).	
3.3	RoHS 2002/95/EC compliant	
3.4	Total number of fibers shall be 6, with 1 loose tubes (Gel Free), each having 6 fibers.	
3.5	The Fiber shall have HDPE/MDPE outer jacket, with Corrugated Steel Tape Armoring with FRLSZH Sheath as per IEC 60332-3.	
	The Fiber shall be Black in color to ensure UV stabilized.	
	The Fiber shall have Water Swellable Tape & Water Swellable Yarns to protect the fiber cores from water.	
3.6	Maximum Cable Diameter shall be 13 ± 5 % with a Cable Weight of 150 kg/km ± 10%.	
3.7	The Tensile Load should be from 2200 N to 2700 N.	
	Central strength member shall be FRP Rod.	
3.8	The Fiber shall be suitable for Aerial (lashed), Indoor and Outdoor Ducts or Direct Burial applications.	
	The Installation Temperature shall be -20 degree Celsius to +70 degree Celsius, Operating Temperature shall be -20 degree Celsius to +70 degree Celsius.	
3.1	The maximum attenuation shall be 0.22 dB/km @ 1550 nm, 0.31 dB/km @ 1380 - 1386 nm and 0.34 dB/km @ 1310 nm.	
	The Chromatic Dispersion @ 1310 nm ps/nm x km $\leq$ 3.5 & @ 1550 nm ps/nm x km $\leq$ 18	
	The maximum cabled cutoff wavelength shall be 1260 nm.	

F.10	12 port LC Single Mode OS2 intelligent loaded LIU	
S. No.	**Description**	**Compliance**
6.1	Shall accommodate 4 coupler plates or 4 pigtail cassettes for a total of 48 fiber terminations.	
6.2	The width shall be 19 inches and height of 1U (1.75 inches), with a maximum of 20-inch depth.	
6.3	The shelf/LIU shall be sliding, and LIU material should be steel.	
6.4	The Fiber shelf must be intelligent ready and must support field upgrade to intelligent fiber panels without removal of existing patch cords and without disruption of network services.	
6.5	Shall have splice trays to splice minimum 32 fibers.	
6.6	Each module shall accommodate 12/24 fibers, with 12/24 LC adapters.	
6.7	The adapter module shall be intelligent upgradable without any interruption to service due to patch cord removal or through re-splicing. The module should only accept standard patch cords and no 9^{th} pin, RFID, CPID etc. will be accepted.	
6.8	The adapter color shall be blue for Single mode.	

F.11	12 Core Single Mode	
S. No.	Description	Compliance
2.1	Shall be Single mode (OS2), FRLSZH Single Jacket, Single Armor, Gel-free, Fiber Cable.	
2.2	Applicable Qualification Standards shall be EN 187105, EN 50173 and Telcordia GR-20 & GR-409.	
	Standards Compliance: ITU-T G.652.D, ITU-T G.657.A1 (bend insensitive) and ANSI/TIA-568 C.3 (OS2).	
2.3	RoHS 2002/95/EC compliant	
2.4	Total number of fibers shall be 12, with 2 loose tubes (Gel Free), each having 6 fibers.	
2.5	The Fiber shall have HDPE/MDPE outer jacket, with Corrugated Steel Tape Armoring with FRLSZH Sheath as per IEC 60332-3.	
	The Fiber shall be Black in color to ensure UV stabilized.	
	The Fiber shall have Water Swellable Tape & Water Swellable Yarns to protect the fiber cores from water.	
2.6	Maximum Cable Diameter shall be 13 ± 5 % with a Cable Weight of 150 kg/km ± 10%.	
2.7	The Tensile Load should be from 2200 N to 2700 N.	
	Central strength member shall be FRP Rod.	
2.8	The Fiber shall be suitable for Aerial (lashed), Indoor and Outdoor Ducts or Direct Burial applications.	
	The Installation Temperature shall be -20 degree Celsius to +70 degree Celsius, Operating Temperature shall be -20 degree Celsius to +70 degree Celsius.	
2.9	The maximum attenuation shall be 0.22 dB/km @ 1550 nm, 0.31 dB/km @ 1380 - 1386 nm and 0.34 dB/km @ 1310 nm.	
	The Chromatic Dispersion @ 1310 nm ps/nm x km $\leq$ 3.5 & @ 1550 nm ps/nm x km $\leq$ 18	
	The maximum cabled cutoff wavelength shall be 1260 nm.	

F.12	24U Outdoor distribution Cabinet	
S. No.	Description	Compliance
1	Standard as per solution Requirement	

F.13	06 Meter I-type pole	
S. No.	Description	Compliance
1	Standard as per solution Requirement	

F.14	05 Meter cantilever pole	
S. No.	Description	Compliance
1	Standard as per solution Requirement	

F.15	Surge Protection Device	

S. No.	Description	Compliance
1	Standard as per solution Requirement	

F.16	10KVA UPS		
S.No	Parameter	Specification	Compliance
1.	Capacity	10 KVA	
2.	Technology	IGBT (Rectifier & Inverter both); ECO Mode required with Inbuilt Isolation Transformer	
3.	Wave form & Freq converter	Pure Sine wave & shall have frequency converter mode	
4.	Display	LCD	
5.	Input power factor correction	0.99 at 100% Linear load	
6.	Input configuration	3Ph, L-N+PE, +/- 10% on full load	
7.	Isolation Transformer	UPS Shall have inbuilt Input Isolation Transformer	
8.	Frequency(Input)	45 to 55 Hz frequency (or 54 to 66 Hz for 60Hz Output)	
9.	Frequency(output)	50Hz or (selectable to 60Hz)	
10.	Output Voltage	220/230/240Vac shall be available with +/-1% regulation	
11.	Output Voltage Distortion	< = 3% max full linear load	
12.	Output Power factor	0.9	
13.	Crest factor	3 or better	
14.	AC-AC Efficiency	Online Mode: Greater than or equal to 88% @ Full Rated Load & Battery Fully charged	
15.	Transfer time Main-Battery	0	
16.	Transfer time Inverter-Bypass	4 msec	
17.	Output Connection	Hardwired Terminal Block required	
18.	Monitoring software for UPS	Shall be provided for monitoring of UPS from remote along with SNMP Card, this project being of high security & safety	
19.	Communication	SNMP	

20.	Port	RS 232	
21.	Battery Type	12V SMF.	
22.	Battery backup	10KVA UPS with 60 min battery backup at 70% load (9984 VAH or more)	
23.	Charger	Shall be minimum 10% of the offered Battery AH	
24.	Battery Flexibility	Required	
25.	Environmental Parameter		
A	Operating temperature range	0-40 deg C	
B	Other	Indication required -> Over Temperature, Load on Battery, Battery low, Mains ON	
C	Humidity	5% to 95% no-condensing	
D	Noise Level	70 dBA max.	
E	EPO	Shall be available	
F	Protection	IP20	

F.17	Outdoor fibre splice Box	
S. No.	Description	Compliance
1	Standard as per solution Requirement	

F.18	Pole Mount Junction Box	
S. No.	Description	Compliance
1	Standard as per solution Requirement	

F.19	3Core 2.5 Sq.mm. Copper cable	
S. No.	Description	Compliance
1	Standard as per solution Requirement	

F.20	3Core 10 Sq.mm	
S. No.	Description	Compliance
1	Standard as per solution Requirement	

F.21	12 port LC Single Mode OS2 intelligent loaded LIU	
S. No.	Description	Compliance
6.1	Shall accommodate 4 coupler plates or 4 pigtail cassettes for a total of 48 fiber terminations.	
6.2	The width shall be 19 inches and height of 1U (1.75 inches), with a maximum of 20-inch depth.	
6.3	The shelf/LIU shall be sliding, and LIU material should be steel.	
6.4	The Fiber shelf must be intelligent ready and must support field upgrade to intelligent fiber panels without removal of existing patch cords and without disruption of network services.	
6.5	Shall have splice trays to splice minimum 32 fibers.	
6.6	Each module shall accommodate 12/24 fibers, with 12/24 LC adapters.	
6.7	The adapter module shall be intelligent upgradable without any interruption to service due to patch cord removal or through re-splicing. The module should only accept standard patch cords and no 9th pin, RFID, CPID etc. will be accepted.	
6.8	The adapter color shall be blue for Single mode.	

F.22	Cat-6 Outdoor UTP Cable	
S. No.	Description	Compliance
I	Category 6 (CAT 6) shall be **23 AWG**, 4 Pair UTP, Outdoor Double Jacketed with Inner Sheath PE and Outer Sheath on LSZH, UV Stabilized Jacket and cable shall comply with ANSI/TIA-568-C.2 standard.	
1	The cable should be in Black color and packaged as reel-in-box.	
2	**Technical Specifications. The broad technical specifications are given below: -**	
2.1	Materials.	
2.2	Conductors: 23 AWG (0.554mm) solid bare copper.	
2.3	Insulation: High Density Polyethylene.	
2.4	Inner Sheath: PE.	
2.5	Outer Sheath Material: LSZH, UV Stabilized & Anti Rodent	
2.6	Diameter: 7.2 mm nom.	
3	**Electrical Characteristics.**	
3.1	Conductor resistance: 9.38 Ω/100m max.	
3.2	Mutual capacitance: 5.6 nF max/100 m.	
3.3	Resistance Unbalance: 5% max.	
3.4	Capacitance unbalance: 330 pF max/100 m.	
3.5	Delay Skew: 45 ns/100 m max. @250 MHz	
4	**Mechanical Characteristics.**	
4.1	Bending Radius: < 28mm	

4.2	Pulling Force: < 14kg.	
4.3	Temperature Range: - 20 deg.C. to +70 deg. C.	

	LAN Cabling Accessories along with Cat-6 UTP Cable	
S. No.	**Description**	**Compliance**
1	Cat 6 UTP Jack PCB based Information Outlet (I/O) RJ45, TIA-568 C.2 Category-6. UL Listed, ETL Channel test report as per ISO/IEC 11801, ANSI/TIA 568 C.2.	
2	high-impact, flame-retardant, UL- RATED 94v 0 thermoplastic – ABS, Plug Insertion Life Min. 750 times as per IEC 60603-7	
3	Contact Resistance: 100 milli ohms; Insulation resistance 500 Mega ohms minimum ;Current Rating : 1.5 A (max) , Contact : 50 micron gold plating over 100 micron nickel underplate.	
4	The information outlet must support 90-degree cable termination. Plug Retention Force: 133 N minimum between modular plug and jack, Meets and exceeds ISO 9001:2015, RoHS compliant.	
5	Cat 6 UTP Jacks should be available in different colors for easy identification.	

F.23	**Outdoor required RJ45 Connector for Wi-Fi & CCTV Cable connector**	
S. No.	**Description**	**Compliance**
1	Cat 6 Ceiling Connector module for connect the devices in the ceiling, i.e., Wi-Fi & IP Cameras	
2	The module shall consist of a connector kit and an 18" CAT 6 solid copper cable. The end of the copper cable shall have a factory terminated RJ 45 plug.	
3	The Cable jacket material of the cable shall be LSZH. The material of the connector kit shall be High-impact, flame retardant, thermoplastic.	
4	Safety compliance: ETL Listed.	
5	The storage temperature shall be 14°F to 140°F (-10°C to 60°C). The operating temperature shall be -40°F to 158°F (-40°C to 70°C).	
6	Shall supports IEEE 802.3af, 802.3at and proposed 802.3bt PoE applications.	

F.24	**Outdoor Faceplate**	
S. No.	**Description**	**Compliance**
1	Shall be available in 1 port, 2 port and 4 port square versions.	
2	General Specifications	
	a) Color: White	
	b) Width: 86.36 mm (3.4 in)	
	c) Height: 86.36 mm (3.4 in)	
	d) Depth: 13.72 mm (0.54 in)	

3	Shall have spring shuttered front access for preventing ingress of dust, shall have no connection with the performance of the jack, RoHS Compliant.	

F.25	Cat 6, UTP, Outdoor Copper Patch Cord	
S. No.	Description	Compliance
1	1, 2-, 3-, 7- & 10-Feet Cat 6 U/UTP Patch Cable, TIA- 568C Category-6, UL-listed / ETL Channel test report as per ISO/IEC 11801, ANSI/TIA 568 C.2, RoHS Compliant.	
2	Patch cords shall be of stranded copper cable with UL/ETL Listed. Conductor Material should be Tinned copper, Plugs shall be designed with an anti-snag latch.	
3	Patch cords sheath shall be LSZH as per IEC 60332-1, IEC 60754-2, IEC 61034-2, Operational Temp: -20º to 60º Celsius	
4	Plug Insertion Life Min. 750 times, Plug Retention Force, Min. 133 N	

F.26	50MM HDPE	
S. No.	Description	Compliance
1	Standard product as per solution requirement preferably Railway/RDSO/DoT approved specifications	

F.27	42U Network Rack	
S. No.	Description	Compliance
1	The racks should be designed to provide a secure, managed environment for server and Networking equipment.	
2	The racks should be UL Listed and India equivalent for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard 19" rack mount equipment.	
3	Front Glass door and Back doors should be perforated with 63% or higher perforations.	
4	Racks should have a provision for cable entry from the top and bottom.	
5	The racks should be available with a vertical equipment mounting space of 42U and each U position should be marked with its numbering.	
6	The vertical mounting rails should have two sets of EIA mounting holes perpendicular to the primary mounting holes to allow devices to be mounted in the side channel.	
7	The unit should include requisite sets of M6 caged nuts, bolts and cup washers, and caged nut tool for the mounting of equipment inside the unit.	
8	Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools. The front door of unit should be reversible so that it may open from either side.	
9	The front and rear doors should open a minimum of 120 degrees to allow easy access to the interior.	
10	All weight bearing components should be constructed from steel with a thickness no less than 0.9mm (20 gauge).	

11	All enclosure panels and rack-mounted equipment should be inherently earthed or grounded directly to the frame.	
12	The racks should have a minimum of IP 20 rating for protection against touch, ingress of foreign bodies, and ingress of water.	
13	Front and Rear mounting rails should he adjustable for depth.	
14	The roof of the racks should be removable from the interior of the enclosure without tools.	
15	The rack units should have mounting provisions for optional door alarm switch to monitor access to the enclosure doors.	
16	The access to racks should have the standard lock and key mechanism.	
17	All racks should also be provided with provision for mounting of Power Distribution Units (PDUs) enabled with modular power strips.	
18	Server Racks should be of 600 mm wide and minimum 1200 mm deep with caster wheels for easy movement and leveling feet	
19	Network Racks should be of 800 mm wide and minimum 1000 mm deep with caster wheels for easy movement and leveling feet	
20	Each Racks should be provided with minimum 20 nos of blanking panels to avoid air recirculation and bypass.	
21	Each Rack should be provided with minimum two temperature and humidity sensor to monitor temperate of Rack Air Inlet and exhaust air.	
22	Racks should be capable to take the server weight of UDL 1360 Kgs and Rolling Load of 1000 Kgs.	
23	All the Racks should be provided with removable side panels.	
24	Each Server Rack should be provided with two zero U Rack Power Distribution Unit. Qty of the PDU should be as per quantity of schedule.	

F.28	42U Server & Storage	
S. No.	Description	Compliance
1	The racks should be designed to provide a secure, managed environment for server and Networking equipment.	
2	The racks should be UL Listed and India equivalent for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard 19" rack mount equipment.	
3	Front Glass door and Back doors should be perforated with 63% or higher perforations.	
4	Racks should have a provision for cable entry from the top and bottom.	
5	The racks should be available with a vertical equipment mounting space of 42U and each U position should be marked with its numbering.	
6	The vertical mounting rails should have two sets of EIA mounting holes perpendicular to the primary mounting holes to allow devices to be mounted in the side channel.	
7	The unit should include requisite sets of M6 caged nuts, bolts and cup washers, and caged nut tool for the mounting of equipment inside the unit.	
8	Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools. The front door of unit should be reversible so that it may open from either side.	
9	The front and rear doors should open a minimum of 120 degrees to allow easy access to the interior.	
10	All weight bearing components should be constructed from steel with a thickness no less than 0.9mm (20 gauge).	

11	All enclosure panels and rack-mounted equipment should be inherently earthed or grounded directly to the frame.	
12	The racks should have a minimum of IP 20 rating for protection against touch, ingress of foreign bodies, and ingress of water.	
13	Front and Rear mounting rails should he adjustable for depth.	
14	The roof of the racks should be removable from the interior of the enclosure without tools.	
15	The rack units should have mounting provisions for optional door alarm switch to monitor access to the enclosure doors.	
16	The access to racks should have the standard lock and key mechanism.	
17	All racks should also be provided with provision for mounting of Power Distribution Units (PDUs) enabled with modular power strips.	
18	Server Racks should be of 600 mm wide and minimum 1200 mm deep with caster wheels for easy movement and leveling feet	
19	Network Racks should be of 800 mm wide and minimum 1000 mm deep with caster wheels for easy movement and leveling feet	
20	Each Racks should be provided with minimum 20 nos of blanking panels to avoid air recirculation and bypass.	
21	Each Rack should be provided with minimum two temperature and humidity sensor to monitor temperate of Rack Air Inlet and exhaust air.	
22	Racks should be capable to take the server weight of UDL 1360 Kgs and Rolling Load of 1000 Kgs.	
23	All the Racks should be provided with removable side panels.	
24	Each Server Rack should be provided with two zero U Rack Power Distribution Unit. Qty of the PDU should be as per quantity of schedule.	

F.29	12-Fiber Single mode MPO12 (Pinned) to MPO12 (Pinned)	
S. No.	Description	Compliance
1	Specifications as mentioned in detailed description in SOR F.29	

F.30	12-Fiber Single mode MPO12 (Pinned) to MPO12 (Pinned)	
S. No.	Description	Compliance
1	Specs is already mentioned in detailed description in SOR F.30	

F.31	19" Rack Mount 1U modular cassette sliding Panel	
S. No.	Description	Compliance
1	Specs is already mentioned in detailed description in SOR F.31	

F.32	Single mode MPO-12 Distribution Module	
S. No.	Description	Compliance

1	Specs is already mentioned in detailed description in SOR F.32	

F.33	Modular Panel Blank Adapter Pack	
S. No.	Description	Compliance
1	Specs is already mentioned in detailed description in SOR F.33	

F.34	Single mode, LC/UPC Uniboot to LC/UPC Uniboot Length 3 meter	
S. No.	Description	Compliance
1	1, 2-, 3-, 7- & 10-Feet Cat 6 U/UTP Patch Cable, TIA- 568C Category-6, UL-listed / ETL Channel test report as per ISO/IEC 11801, ANSI/TIA 568 C.2, RoHS Compliant.	
2	Patch cords shall be of stranded copper cable with UL/ETL Listed. Conductor Material should be Tinned copper, Plugs shall be designed with an anti-snag latch.	
3	Patch cords sheath shall be LSZH as per IEC 60332-1, IEC 60754-2, IEC 61034-2, Operational Temp: -20º to 60º Celsius	
4	Plug Insertion Life Min. 750 times, Plug Retention Force, Min. 133 N	

F.35	Single mode, LC/UPC Uniboot to LC/UPC Uniboot Length 5 meter	
S. No.	Description	Compliance
1	1, 2-, 3-, 7- & 10-Feet Cat 6 U/UTP Patch Cable, TIA- 568C Category-6, UL-listed / ETL Channel test report as per ISO/IEC 11801, ANSI/TIA 568 C.2, RoHS Compliant.	
2	Patch cords shall be of stranded copper cable with UL/ETL Listed. Conductor Material should be Tinned copper, Plugs shall be designed with an anti-snag latch.	
3	Patch cords sheath shall be LSZH as per IEC 60332-1, IEC 60754-2, IEC 61034-2, Operational Temp: -20º to 60º Celsius	
4	Plug Insertion Life Min. 750 times, Plug Retention Force, Min. 133 N	

F36-41	Specification for SOR Item F.36-41	
S. No.	Description	Compliance
11.1	System shall have single tier distributed architecture (single controller vs. cascading/multi-tier controllers, single controller is capable to communicate to intelligent patch panels directly).	
11.2	System shall require only three components for system design:	
	Intelligent patch panels, single system controller and software.	
11.3	System shall provide full featured electronic work order capabilities that include:	
11.4	The solution should provide information of the rack layout in graphical view and allow interaction with displayed information in real time (e.g. lighting an LED over a panel port remotely). This is extremely important for remote site management.	
11.5	The solution should have the capability to create and assign work orders to technicians. It should –	

	Ensure the ability to create, assign and monitor the status of any work order to any technician.	
	Warn of a mismatch between requested activity and real status through ongoing scanning activity and LED guidance. Automatically update the database upon completion of task.	
11.6	The solution should be capable to collect information of the activity at each switch port & identify unused switch ports. This is necessary to optimize the usage of switch ports.	
11.7	The solution should come with a built-in graphical view capability of the complete floor plans and should be able to import files in any of the following formats: jpeg, bmp or dwg. This should show the geographical locations of each asset in the entire network.	
11.8	The Intelligent Physical Layer Management Solution should have guidance lights per port. The light guidance is mandatory for tracing the two ends of any patch cord, executing planned work orders and for remote management.	
11.9	The Intelligent System Controller shall have a feature to lock the screen and can be activated or used only using a unique pin number. This is to provide enhanced security so that no unauthorized access can happen via the controller.	
11.1	System shall be capable to support cross-connect as well as interconnect administration topology.	
11.11	System support for interconnect topology shall be enabled without a need for special accessories to be installed on managed network equipment.	
11.12	The Controller shall have the option of a redundant power supply, i.e., it should have the option of dual power supply.	
11.13	System shall enable full-featured remote administration capabilities either via a software client or a web client that include electronic work orders, database access, etc.	
11.14	System shall be able to generate real-time security alerts upon:	
	a) Insertion of a plug into intelligent panel port	
	b) Removal of a plug from intelligent panel port	
	c) Pressing of a trace button above panel port	
	d) Unauthorized MAC activity in a telecom room	
11.15	The Software shall be capable of importing, displaying and printing CAD drawings for accurate representation of building's floor plans.	
11.16	The Software shall have capability to auto discover the installed intelligent hardware (intelligent panels and control systems) in each rack/cabinet and to auto populate this information in its database.	
11.17	The Software shall provide the capability to allow external Software systems (for example Aperture, Remedy Helpdesk, HP Service Manager, etc.) to interact with the AIM Software.	
11.18	Intelligent pre-terminated fiber shelves shall be available in high density configurations providing support up to 144 -duplex LC ports in 2U or more as well as in 4U configuration supporting up to 244 duplex LC ports or more.	
11.19	The Solution must support field upgrade of intelligence-ready passive copper and fiber panels without removal of existing patch cords and without disruption of network services due to the high criticality of the Data Center. That is, all non-intelligent panels should be upgradable to intelligent panels without any patch cord disconnection or removal.	
11.2	If the need arises all the controllers in a single room should function on only one Switch Port per Zone/DC Room.	
11.21	Shall comply to ISO/IEC 18598 Information technology -- Automated infrastructure management (AIM) systems.	

Note:

1. Bidder should clearly mention complied or not complied against each item in above technical compliance sheet. No cell should be left blank.
2. All features / functionality / protocols which are mentioned as "... should support" shall imply that the same is available and enabled for use from day 1 without any additional financial implication.
3. All the OEMs quoted should have TAC Center in India along with Toll-Free Number, etc..

****

(END OF EOI/RFP DOCUMENT)