RAILTEL CORPORATION OF INDIA LIMITED
(A Govt. of India Undertaking)

Expression of Interest for Selection of Partner from Empaneled Business Associates

For

"Supply, Installation, Configuration, Commissioning & Integration Of ICT Infrastructure For End Customer Data Centre Along With It's Operation And Maintenance.**"**

EOI No: RailTel/EOI/COMKTG/EB/C-DC/2024-25/08 dated 16th June 2024

EOI NOTICE

Plate-A, 6th Floor, Office Tower-2, NBCC Building, East Kidwai Nagar, New Delhi-110023

EOI Notice No: RailTel/EOI/COMKTG/EB/C-DC/2024-25/08 dated 16th June 2024

RailTel Corporation of India Ltd., (here after referred to as "RailTel") invites EOIs from RailTel's Empaneled Partners for the selection of suitable partner for **"Supply, installation, configuration, commissioning & integration of ICT infrastructure for End Customer Data Centre along with it's operation and maintenance".**

The details are as under:

1	Last date for submission of Technical Packet against EOIs by bidders	20th June 2024 at 15:00 Hours
2	Opening of Technical Bid of EOIs	20th June 2024 at 15:30 Hours
3	Number of copies to be submitted for scope ofwork	One (Single stage Two packet system) Only PQ/Technically qualified bids shall be eligible for financial bid evaluation.
4	EOI fees inclusive tax (Non-refundable)	Rs. 5,000/- (Five Thousand only)
5	EMD	Rs. ₹ 73,30,000/- (Rupees Seventy three Lakh thirty Thousand Only) to be submitted along with EOI. To be submitted by selected Business Associate, in the form of BG/online transfer. *BG as EMD validity: Bid validity period + 2 months and claim period of 1 year from BG expiry period. (SFMS report guidelines: - BG advising message – IFN 760COV/ IFN 767COV via SFMS • To mandatorily send the Cover message at the time of BG issuance. • IFSC Code of ICICI Bank to be used (ICIC0000007). • Mention the unique reference (RAILTEL6103) in field 7037.)
6	Bid Submission Mode	Online on https://railtel.enivida.com

The EMD should be in the favor of RailTel Corporation of India Limited payable at Delhi through online bank transfer or EMD can be submitted as PBG in favor of RailTel Corporation of India Limited. Partner

needs to share the online payment transfer details like UTR No. date and Bank along with the proposal.

RailTel Bank Details: Union Bank of India, Account No. 340601010050446, IFSC Code - UBIN0534064.
Offers not accompanied with EMD shall be summarily rejected.

iii. The EMD may be forfeited if a bidder withdraws or amends its/his EoI or impairs or derogates from the EoI in any respect within the period of validity of the EoI or in the case of a successful bidder, if the bidder fails to accept the Purchase order/LOA or fails to furnish performance bank guarantee (security deposit).

Eligible Business Associates are required to direct all communications related to this Invitation for EoI document, through the following Nominated Point of Contact persons:

Contact person : Hemant Yadav
Designation: Jt.GM/Govt. Business
Email: hemantyadav@railtelindia.com
Mob: 9717644137

Note:

1. The EOI response is invited from eligible **Empaneled Partners of RailTel only.**
2. The Bidders has to submit their response in form of duly signed and stamped and **submit techno-commercial bid at the E-nivida portal through Online mode**, within the stipulated date and time, as mentioned in this EOI document.
3. The interested bidders has to submit the EOI fees, EMD, and Non Disclosure Undertaking (NDU), OEM technical solution as per the format given at Annexure-7 of this EOI along with their technical bid.
4. The selected bidder will have to accept all Terms & Conditions of End Customer RFP on back-to-back basis.
5. All the document must be submitted with **proper indexing** and **page nos.**
6. Bidders has to agree to comply with all OEM technical & financial documentation, Technical certificates/others as per end-to-end customer requirement mentioned in the end customer's RFP enclosed along with this EoI.
7. Bidders also undertake to submit OEMs solution and other documents required in the end Customer Organization's tender in favour of RailTel against the proposed products and solutions. The offers of the bidders who qualify the PQ and TQ criteria shall enter into the next stage of financial bid evaluation.

8. This is an **exclusive partnership arrangement with empaneled business associate of RailTel for " Supply, installation, configuration, commissioning & integration of ICT infrastructure for End Customer Data Centre along with it's operation and maintenance".**

9. **Transfer and Sub-letting**. The Business Associate has no right to give, bargain, sell, assign or sublet or otherwise dispose of the Contract or any part thereof, as well as to give or to let a third partytake benefit or advantage of the present Contract or any part thereof.

10. No exemption/relaxation is applicable to MSME/Startups.

1. Introduction about RailTel

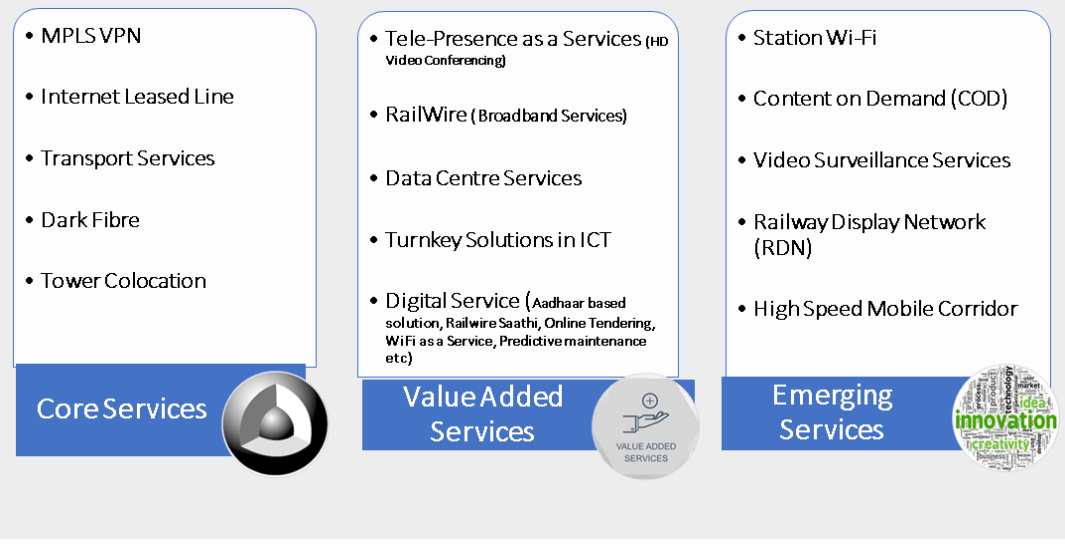
RailTel Corporation of India Limited (RailTel), an ISO-9001:2000 organization is a Mini Ratna Government of India undertaking under the Ministry of Railways. The Corporation was formed in Sept 2000 with the objectives to create nationwide Broadband Telecom and Multimedia Network in all parts of the country, to modernize Train Control Operation and Safety System of Indian Railways and to contribute to realization of goals and objective of national telecom policy 1999. RailTel is a wholly owned subsidiary of Indian Railways.

RailTel has approximately 61000 kms of OFC along the protected Railway tracks. The transport network is built on high capacity DWDM and an IP/ MPLS network over it to support mission critical communication requirements of Indian Railways and other customers. RailTel has Tier-III Data Center in Gurgaon and Secunderabad hosting / collocating critical applications. RailTel is also providing Telepresence as a Service (TpaaS), where a High Definition Video Conference facility bundled with required BW is provided as a Service.

For ensuring efficient administration across India, country has been divided into four regions namely, Eastern, Northern, Southern & Western each headed by Executive Director and Headquartered at Kolkata, New Delhi, Secunderabad & Mumbai respectively. These regions are further divided into territories for efficient working. RailTel has territorial offices at Guwahati, & Bhubaneswar in East, Chandigarh, Jaipur, Lucknow in North, Chennai & Bangalore in South, Bhopal, and Pune & Ahmedabad in West. Various other territorial offices across the country are proposed to be created shortly.

RailTel's business service lines can be categorized into three heads namely B2G/B2B (Business to Government and Business to Business) and B2C (Business to customers):

Licenses & Service portfolio:
Presently, RailTel holds Infrastructure Provider -1, National Long Distance Operator, International Long Disftance Operator and Internet Service Provider (Class-A) licenses under which the following services are being offered to various customers:



a) Carrier Services

- National Long Distance: Carriage of Inter & Intra -circle Voice Traffic across India using state of the art NGN based network through its Interconnection with all leading Telecom Operators
- Lease Line Services: Available for granularities from E1 to multiple of Gigabit bandwidth& above
- Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks
- Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

b) Enterprise Services

- Managed Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
- MPLS VPN: Layer-2 & Layer-3 VPN available for granularities from 2 Mbps& above
- Dedicated Internet Bandwidth: Experience the "Always ON" internet connectivity at your fingertips in granularities 2 Mbps to several Gbps

c) DATA CENTER Infrastructure as a services (IaaS), Hosting as Services, Security operation Centre as a Service (SOCaaS): RailTel has MeitY empaneled two Tier-III data centres in Gurgaon & Secunderabad. Presently RailTel is hosting critical applications of Indian Railways, Central & State government/ PSUs applications. RailTel will facilitate Government's applications / hosting services including smooth transition to secured state owned RailTel's Data Centers and Disaster Recovery Centres. RailTel also offers SOC as a Service 'SOCaaS'. In addition, RailTel offers VPN client services so that employees can seamlessly access government's intranet, applications securely from anywhere without compromising security.

- National Long Distance: Carriage of Inter & Intra -circle Voice Traffic across India using state of the art NGN based network through its Interconnection with all leading Telecom Operators
- Lease Line Services: Available for granularities from E1 to multiple of Gigabit bandwidth& above
- Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks
- Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

d) High-Definition Video Conference: RailTel has unique service model of providing high definition video conference bundled with Video Conference equipment, bandwidth and FMS services to provide end to end seamless services on OPEX model connecting HQ with other critical offices. RailTel also offers application-based video conference solution for employees to be productive specially during this pandemic situation.

e) Retail Services – RailWire

RailWire: Triple Play Broadband Services for the Masses. RailTel has unique model of delivering broadband services, wherein local entrepreneurs are engaged in delivering &

maintaining broadband services and up to 66% of the total revenues earned are shared to these local entrepreneurs in the state, generating jobs and revitalizing local economies. On date RailTel is serving 7nautho. 5,00,000 subscribers on PAN Indian basis. RailTel can provide broadband service across– Government PSU or any organization's officers colonies and residences.

2. Project Background and Objective of EOI

RailTel intends to select a suitable partner for **" Supply, installation, configuration, commissioning & integration of ICT infrastructure for End Customer Data Centre along with it's operation and maintenance".**

RailTel invites EOIs from RailTel's Empaneled Partners for the selection of suitable partner for **" Supply, installation, configuration, commissioning & integration of ICT infrastructure for End Customer Data Centre along with it's operation and maintenance".**The empaneled partner is expected to have excellent execution capability and good understanding customer local environment.

3. Scope of Work:

RailTel intends to explore and select a suitable partner for **" Supply, installation, configuration, commissioning & integration of ICT infrastructure for End Customer Data Centre along with it's operation and maintenance".**

The brief scope of work is provided below for reference: -

The overall scope of work as mentioned in the customer RFP can be divided into 2 parts viz.

1. Supply, installation, configuration, commissioning & integration of ICT infrastructure.
2. Operation and Maintenance of the ICT infrastructure in compliance with the SLA as defined in Sr. No 5 of the customer RFP.

The brief scope of work as mentioned in the customer RFP is defined below:

1. Installation and commission the required IT hardware assets and software components into the racks at End Customer Data Centre, New Delhi.
2. The selected SI shall centrally monitor and manage the devices & solutions on a 24x7x365 basis to ensure an uptime of 99.98% for all the ICT infrastructure**.**
3. SI shall position a dedicated technical onsite team to implement, commission and manage the ICT infrastructure deployed in in accordance with the necessary security policies and issued guidelines by End Customer time to time.

4. The onsite team deployed by the MSP/SI shall regularly monitor and troubleshoot the ICT infrastructure in compliance with the SLA as defined in Sr. No. 5 of the customer RFP.

5. The SI shall ensure that the Standard operating Procedures, policies and guidelines etc. for the data centre is fully compliant to the latest certification requirements of ISO 20000, ISO 27001, ISO 22301, ISO 27701, ISO 27017 etc. End Customer may hire an auditing agency through a separate process for conducting various audits. During the audit if that agency identifies any shortcoming/ lack of compliance, the SI shall extend all kind of assistance in removing shortcoming/ lack of compliance in consultation with End Customer.

6. For detailed requirement specifications for each of the hardware and software components, please refer to Annexure: Technical Specification of the customer RFP which is attached herewith

I. The Detailed specification and scope of work is mentioned in customer RFP which is placed at **Appendix-A.**

The above scope of work is indicative and the detailed scope of work is given in the end customer RFP with latest amendments and clarifications.

In case of any discrepancy or ambiguity in any clause / specification pertaining to scope of work area, the RFP released by end customer organization shall supersede and will be considered sacrosanct. (All associated clarifications, response to queries, revisions, addendum and corrigendum also included.)

Business associate can participate as a sole bidder only and consortium is not allowed.

Special Note: Through this EOI RailTel is proposed to explore possible solution provider among its empaneled business partners, with competitive commercials. However, RailTel may retain any portion of the work mentioned in the BOQ, where RailTel has competence so that overall proposal becomes most economically viable.

4. Response to EOI guidelines

4.1 Language of Proposals

The proposal and all correspondence and documents shall be written in English in soft copy through an email.

4.2 RailTel's Right to Accept/Reject responses

RailTel reserves the right to accept or reject any response and annul the bidding process or even reject all responses at any time prior to selecting the partner, without thereby incurring any liability to the affected bidder or Business Associate or without any obligation to inform the affected bidder or bidders about the grounds for RailTel's action.

4.3 EOI response Document.

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Submission of bids, not substantially responsive to the bidding document in every aspect will be at the bidder's risk and may result in rejection of its bid without any further reference to the bidder.

All pages of the documents shall be signed by the bidder including the closing page in token of his having studied the EOI document and should be submitted along with the bid.

4.4 Period of Validity of bids and Bid Currency

Bid of Interested partners shall remain valid for the period of 45 days from the last date of submission of EOI, as mentioned in this EOI document.

RailTel may request for an extension of the period of validity of bids. The validity of the 'EMD', should also be suitably extended if called upon to do so by RailTel. 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.

4.5 Bidding Process

The bidding process as defined in para 4.10 & 6.

4.6 Bid Earnest Money (EMD)

4.6.1 The Business Associate shall furnish a sum as given in EOI Notice via online transfer from any scheduled bank in India in favour of "RailTel Corporation of India Limited"along with the offer. This will be called as **EMD.**

4.6.2 Offers not accompanied with valid EOI Earnest Money Deposit shall be summarily rejected.

4.6.3 Deleted.

4.6.4 **Return of EMD for unsuccessful Business Associates:** EOI EMD of the unsuccessful Business Associate shall be returned without interest after completion of EOI process.

4.6.5 **Return of EMD for successful Business Associate:** Earnest Money Deposit (EMD) if applicable of the successful bidder will be discharged / returned as promptly as possible after the receipt of RailTel's EMD/BG from the Customer and or on receipt of Security Deposit Performance Bank Guarantee as applicable (clause no. 4.7) from Business Associate whichever is later.

4.6.6 **Forfeiture of EMD and or Penal action as per EMD Declaration:**

4.6.6.1 The EMD may be forfeited and or penal action shall be initiated if a Business Associate withdraws his offer or modifies the terms and conditions of the offer during validity period.

4.6.6.2 In case of non-submission of SD/PBG (as per clause no. 4.7) lead to forfeiture of EMD if applicable and or suitable action as prescribed in the EMD Declaration shall be initiated as applicable.

4.7 Security Deposit / Performance Bank Guarantee (PBG)

4.7.1 In case the bid is successful, the PBG of requisite amount proportionate to the agreed scope of the work will have to be submitted to RailTel.

4.7.2 As per work share arrangements agreed between RailTel and Business Associate the PBG will be proportionately decided and submitted by the selected Business Associate i.e 3% of the contract value or as decided by RailTel as per the % of the PBG applicable as per extant rules of PBG in RailTel or as per PBG required by end customer of RailTel.

4.8 Last date & time for Submission of EOI response

EOI response must be submitted to RailTel on E-nivida portal as specified in the preamble not later than the specified date and time mentioned in the preamble.

4.9 Modification and/or Withdrawal of EOI response

EOI response once submitted will be treated as final and no modification will be permitted.

No Business Associate shall be allowed to withdraw the response after the last date and time for submission.

The successful Business Associate will not be allowed to withdraw or back out from the response commitments. In case of withdrawal or backout by the successful business associate, the Earnest Money Deposit shall be forfeited, and all interests/claims of such Business Associate shall be deemed as foreclosed.

4.10 Details of Financial bid for the above referred tender

The offers of the bidders who qualify the PQ and TQ criteria shall enter into the next stage of financial bid opening.

.

Business Associate with the lowest (L1) offer will be selected for " Supply, installation, configuration, commissioning & integration of ICT infrastructure for End Customer Data Centre along with it's

operation and maintenance."

4.11 Clarification of EOI Response

To assist in the examination, evaluation and comparison of bids the purchaser may, at its discretion, ask the Business Associate for clarification. The response should be in writing and no change in the price or substance of the EOI response shall be sought, offered or permitted.

4.12 Period of Association/Validity of Agreement

RailTel will enter into an agreement with selected bidder with detailed Terms and conditions. The terms and conditions of the agreement will be on back to back basis as per end customer RFP and work order placed on RailTel.

5. Eligibility Criteria for Bidding Business Partner of RailTel/OEMs.

S. No.	Particulars	Criteria for Tender Package *(Mandatory Compliance & Document Submission)*
A)	**Financial Conditions**	
i)	Bidder should be registered under Companies Act, 1956 or Companies Act 2013 or as amended and should have at least 3-years of operations in India as on bid submission date and should have a operational office in Delhi/NCR.	1. Certificate of Incorporation 2. GST Registration 3. PAN Card 4. Copy of ITR filed for last 3 financial year ending 31st March 2024.
ii)	Bidder should have average annual turnover of at least INR 62.12 Cr. (exclusive of tax) for last three years (FY 21-22, 22-23, 23-24).	Balance Sheet and Turnover Certificate issued by the Chartered Accountant
iii)	Bidder should also have a positive net worth in the last 3 financial years (FY 21-22, 22-23, 23-24).	**Positive Net Worth Certificate** issued by the CA for the last three financial years (FY 21-22, 22-23, 23-24).
B)	**Technical Conditions**	
iv)	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/ Autonomous Bodies and other organization's in India as: The Bidder should have experience of One similar work of value not less than Rs.37.27 Cr.(Without GST) or The Bidder should have experience of Two similar works each of value not less than Rs.24.85 Cr. (Without GST) or The Bidder should have experience of Three similar works each of value not less than Rs.18.64 Cr. (Without GST) *Similar projects would be Definition of Similar Work: - Works entailing project in the field of NOC / SOC / Data Centre IT Security / IT / IteS/ ICT for any Government department or Public Sector Units or public listed companies.*	Documentary evidence such as Certificate from Customer i.e. purchase orders/ work orders and completion certificate for completed projects. Copy of Purchase/ Work Order & completion certificate issued by customer / PO issuing authority. The bidder must provide details of a personnel for verification purpose at PO/ certificate issuing organization clearly mentioning name of client, designation, contact number and mail ID on bidder's letter head.
v)	Bidder shall have at least 50 technical personnel on its payroll.	Undertaking from authorized signatory or HR Head of the Company on its letter head.
vi)	The bidder must have at least three of the following with the first two certificates being mandatory: a) ISO 27001:2015/2013 b) ISO 20000-1:2018 c) ISO 9001:2015	Copy of any three valid Certificates

S. No.	Particulars	Criteria for Tender Package *(Mandatory Compliance & Document Submission)*
	d) ISO 27017:2015 e) ISO 27018:2019 f) ISO 22301:2019 g) PCI-DSS h) SOC 2 Type 2 audit i) CMMi L3 or above	
vii)	Empanelment with RailTel: Bidder must be empanelled with RailTel as business associate as on date of bid submission.	Copy of Empanelment letter and Empanelment PBG/EMD submitted, if any.
C)	**Annexures**	
vii)	**Annexure 1**	**Covering Letter:** Self-certification duly signed by authorized signatory on company letter head.
viii)	**Annexure 2**	The Bidder should agree to abide by all the technical, commercial & financial conditions of the end customer RFP for which EOI is submitted.
		Self-certification duly signed by authorized signatory on company letter head.
ix)	**Annexure 3**	An undertaking signed by the Authorized Signatory of the company to be provided on letter head. The Bidder should not have been blacklisted/debarred by any Governmental/ Non-Governmental Organization in India as on bid submission date.
x)	**Annexure-4**	Format for Affidavit to be uploaded by bidder with the tender documents.
xi)	**Annexure-5**	Non-disclosure agreement with RailTel.
xii)	**Power of Attorney**	Bidder need to provide Power of Attorney and Board Resolution in favour of one of its employees who will sign the Bid Documents.
xiii)	**Additional Documents to be Submitted**	Technical Proposal with overview of the project with strength of the Partner.
xiv)	**Annexure-6**	EMD (as PBG) Format
xv)	**Annexure-7**	Non-Disclosure Undertaking

6. Bidder's Profile

The bidder shall provide the information in the below table:

S. No.	ITEM	Details
1.	Full name of bidder's firm	
2.	Full address, telephone numbers, fax numbers, and email address of the primary office of the organization / main / head / corporate office	
3.	Name, designation and full address of the Chief Executive Officer of the bidder's organization as a whole, including contact numbers and email Address	
4.	Full address, telephone and fax numbers, and email addresses of the office of the organization dealing with this tender	
5.	Name, designation and full address of the person dealing with the tender to whom all reference shall be made regarding the tender enquiry. His/her telephone, mobile, Fax and email address.	
6.	Bank Details (Bank Branch Name, IFSC Code, Account number)	
7.	GST Registration number	

7. Evaluation Criteria

7.1 The Bidders will be evaluated on the basis of the Eligibility Criteria, TQ as mentioned at para 5. The bidders who qualify these criteria would be eligible to enter the next stage of financial bid opening. The price bid of the bidder fulfilling these eligibility criteria's would be opened and the bidder with lowest overall price as per the BOQ would be declared as L1 bidder and will be considered for awarding the work for the defined scope of work.

7.2 Deleted

7.3 RailTel reserves the right to accept or reject the response against this EOI, without assigning any reasons. The decision of RailTel is final and binding on the participants. The RailTel evaluation committee will determine whether the proposal/ information is complete in all respects and the decision of the evaluation committee shall be final. RailTel may at its discretion assign lead factor to the Business associate/OEM as per RailTel policy for shortlisting partner against this EOI.

7.4 All General requirement mentioned in the Technical Specifications are required to be complied. The solution proposed should be robust and scalable.

8. Payment terms

8.1 RailTel shall make payment to selected Business Associate(s)/OEM after receiving payment from Customer for the agreed scope of work. In case of any penalty or deduction made by customer for the portion of work to be done by BA, same shall be passed on to Business

Associate.

8.2 All payments by RailTel to the Partner will be made after the receipt of payment by RailTel from end Customer organization and after submission of all documents as specified in end customer RFP.

8.3 Payment will be released after receiving the invoice for the work / services and after RailTel has received the payment from the Customer for the same work / services. Any deduction /Penalties levied by Customer on invoices of RailTel will be carried **back-to-back** and will be deducted from selected BA's invoices, subject to the cause to deduction / penalty is due to deviation in terms and conditions of service standards by the BA.

8.4 No advance payment will be given to selected BA if RailTel gets the same from end customer.

8.5 Documents list required at the time of payment/invoice submission by selected bidder shall be: -

i PO copy issued to selected BA.

ii Submission/Declaration of applicable BG amount against PO issued to selectedbidder/ BA.

iii Original Tax Invoice for the period claimed.

iv TDS declaration.

v Three copies of supplier's invoice showing contract number, goods description, quantity, unit price and total amount.

vi Two copies of packing list identifying contents of each package.

vii Inspection and Insurance certificate, if any.

viii Certificate of origin for imported goods Consignee Receipt Certificate in original issued by the authorized User Department representatives/Concerned Stores Representative of the consignee if any.

ix) Photocopy of all documents submitted by RailTel along with their invoice to customer.

9. SLA

The selected bidder will be required to adhere to the SLA matrix as defined in the end Customer organization tender for his scope of work and the SLA breach penalty will be applicable proportionately on the selected bidder, as specified in the end Customer organization Tender. The SLA scoring and penalty deduction mechanism for in-scope of work area shall be followed as specified in the Tender. All associated clarifications, responses to queries, revisions, addendum and corrigendum, associated Prime Services Agreement (PSA)/ MSA/ SLA also included. Any deduction by Customer from RailTel payments on account of SLA breach which is attributable to Partner will be passed on to the Partner proportionately based on its scope of work.

Note: RailTel reserves the rights to undertake any of the work on it's own as mentioned in the customer BOQ.

Annexure 1: Format for COVERING LETTER

COVERING LETTER (To be on company letter head)

To,

RailTel Corporation of India Ltd.
Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar, New Delhi-110023

Dear Sir,

SUB: Participation in the EoI process

Having examined the Invitation for EoI document bearing the reference number _____ released by your esteemed organization, we, undersigned, hereby acknowledge the receipt of the same and offer to participate in conformity with the said Invitation for EoI document.

If our application is accepted, we undertake to abide by all the terms and conditions mentioned in the said Invitation for EoI document.

We hereby declare that all the information and supporting documents furnished as a part of our response to the said Invitation for EoI document, are true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our EoI is liable to be rejected.

We hereby Submit EMD amount of Rs._____Issued vide_____from Bank_____.

Authorized Signatory
Name
Designation

Annexure 2: Format for Self-Certificate & Undertaking

Self-Certificate (To be on company letter head)

EoI Reference No: Date:

To,

RailTel Corporation of India Ltd.
Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar, New Delhi-110023

Dear Sir,

Sub: Self Certificate for Tender, Technical & other compliances

1) Having examined the Technical specifications mentioned in this EOI & end customer tender, we hereby confirm that we meet all specification.
2) We _____agree to abide by all the technical, commercial & financial conditions of the end customer RFP for which EOI is submitted (except pricing, termination & risk purchase rights of the RailTel). We understand and agree that RailTel shall release the payment to selected partner after the receipt of corresponding payment from end customer by RailTel. Further we understand that in case selected partner fails to execute assigned portion of work, then the same shall be executed by RailTel through third party or departmentally at the risk and cost of selected partner.
3) We agree to abide by all the technical, commercial & financial conditions of the end customer's RFP for the agreed scope of work for which this EOI is submitted.
4) We hereby agree to comply with all OEM technical & Financial documentation including manufacturer authorization form , Technical certificates/others as per end to end requirement mentioned in the end customer's RFP. We are hereby enclosing the arrangement of OEMs against each of the BOQ item quoted as mentioned end customer's RFP. We also undertake to submit including manufacturer authorization form / Engagement document and other documents required in the end Customer organization tender in favour of RailTel against the proposed products.
5) We hereby certify that any services, equipment and materials to be supplied are produced in eligible source country complying with OM/F. No. 6/18/2019 dated 23rd July 2020 issued by DoE, MoF.
6) We hereby undertake to work with RailTel as per end customer's RFP terms and conditions. We confirm to submit all the supporting documents constituting/ in compliance with the Criteria as required in the end customer's RFP terms and conditions like technical certificates, OEM compliance documents (including manufacturer authorization form, technical solution documents etc.)
7) We understand and agree that RailTel is intending to select partner who is willing to accept all terms & conditions of end customer organization's RFP for the agreed scope of work. RailTel will strategies

to retain scope of work where RailTel has competence.

8) We hereby agree to submit that in case of being selected by RailTel as partner for the proposed project (for which EOI is submitted), we will submit all the forms, appendix, relevant documents etc. to RailTel that is required and desired by end Customer as and when required.

9) We hereby undertake to sign Non-Disclosure Agreement with RailTel on a non-judicial stamp paper of Rs. 100/- in the prescribed Format.

10) We undertake that we will not share any information pertaining to this EOI and end customer technical requirements, commercial bid format to any other organization during the evaluation of the EOI process and final selection of the bidder and would keep all these information confidential and would not share the information with anyone.

Authorized Signatory

Name & Designation

Annexure 3: Undertaking for not Being Blacklisted/Debarred

<On Company Letter Head>

To,

RailTel Corporation of India Ltd
Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar, New Delhi-110023

Subject: **Undertaking for not Being Blacklisted/Debarred**

We, <Company>having our registered office at < Company address>, are an established authorized partner cum Company since last <No. of years> and have our registered office at < address of registered office >.
We do here by confirm, that we have read and understood each and every tender terms and conditions of above cited tender and are bidding in complete compliance of all terms & conditions of tender. We understand that it will be our sole responsibility to deliver the product and services as per conditions set out in tender. Any failure at our end will make us liable for penalties as defined in tender and cancelation of empanelment.
We also confirm that every supply will have OEM support pack of five years or as defined in the end customer RFP for back-end support, although we will provide comprehensive warranty as per tender requirement directly.
We will take all necessary steps for successful execution this project as per tender requirements.
We do hereby also confirm that our company has not been blacklisted in any Central / State Government department, public sector undertaking and autonomous body in last three years.

Date and Place

Authorized Signatory's Signature:

Authorized Signatory's Name and Designation:

Bidder's Company Seal:

Annexure 4: Format of Affidavit

(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 BA) **

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

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

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

3. I/we hereby declare that I/we have downloaded the EOI documents from RailTel website www.railtelindia.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 document. In case of any discrepancy noticed at any stage i.e. evaluation of EOI, 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 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, it shall lead to forfeiture of the EOI EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the BA)**_____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.

9. I/we the BA(s) have carefully read and understand terms and conditions of the tender/RFP of CoR /EOI and also accept all the terms and conditions of the tender/RFP/ of CoR / EOI including addendum/corrigendum.

10. I/we understand that we will submit all the required including manufacturer authorization form /documents/annexures as per requirement of tender/RFP of CoR /EOI before reasonable time i.e during our bid submission as conveyed by competent Authority of RailTel.

DEPONENT

SEAL AND SIGNATURE OF THE BA VERIFICATION

I/We above named EOI 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 BA

Place:
Dated:

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

Annexure-5: Non-Disclosure Agreement (NDA) Format

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (this "***Agreement***") is made and entered into on this _____ day of ____ , 2024 (the "***Effective Date***") at_____.

By and between

RailTel Corporation of India Limited, **(CIN: L64202DL2000GOI107905),** a Public Sector Undertaking under Ministry of Railways, Govt. of India, having its registered and corporate office at Plate-A, 6th Floor, Office Block, Tower -2, East Kidwai Nagar, New Delhi-110023, (hereinafter referred to as **'RailTel')**, which expression shall unless repugnant to the context or meaning thereof, deem to mean and include its successors and its permitted assignees of the ONE PART,

And

_____) (CIN:_____), a company duly incorporated under the provisions of Companies Act, _____ having its registered office at _____, (hereinafter referred to as **'_____'),** which expression shall unless repugnant to the context or meaning thereof, deem to mean and include its successors and its permitted assignees of OTHER PART

RailTel and _____ shall be individually referred to as "Party" and jointly as "Parties"

WHEREAS, RailTel and _____, each possesses confidential and proprietary information related to its business activities, including, but not limited to, that information designated as confidential or proprietary under Section 2 of this Agreement, as well as technical and non-technical information, patents, copyrights, trade secrets, know-how, financial data, design details and specifications, engineering, business and marketing strategies and plans, forecasts or plans, pricing strategies, formulas, procurement requirements, vendor and customer lists, inventions, techniques, sketches, drawings, models, processes, apparatus, equipment, algorithms, software programs, software source documents, product designs and the like, and third party confidential information (collectively, the "***Information***");

WHEREAS, the Parties have initiated discussions regarding a possible business relationship for _____.

WHEREAS, each Party accordingly desires to disclose certain Information (each Party, in such disclosing capacity, the "***Disclosing Party***") to the other Party (each Party, in such receiving capacity, the "***Receiving Party***") subject to the terms and conditions of this Agreement.

NOW THEREFORE, in consideration of the receipt of certain Information, and the mutual promises made in this Agreement, the Parties, intending to be legally bound, hereby agree as follows:

1. Permitted Use.

(a) Receiving Party shall:

(i) hold all Information received from Disclosing Party in confidence;

(ii) use such Information for the purpose of evaluating the possibility of entering into a commercial arrangement between the Parties concerning such Information; and

(iii) restrict disclosure of such Information to those of Receiving Party's officers, directors, employees, affiliates, advisors, agents and consultants (collectively, the "***Representatives***") who the Receiving Party, in its reasonable discretion, deems need to know such Information, and are

bound by the terms and conditions of (1) this Agreement, or (2) an agreement with terms and conditions substantially similar to those set forth in this Agreement.

(b) The restrictions on Receiving Party's use and disclosure of Information as set forth above shall not apply to any Information that Receiving Party can demonstrate:

(i) is wholly and independently developed by Receiving Party without the use of Information of Disclosing Party;

(ii) at the time of disclosure to Receiving Party, was either (A) in the public domain, or (B) known to Receiving Party;

(iii) is approved for release by written authorization of Disclosing Party; or

(iv) is disclosed in response to a valid order of a court or other governmental body in the India or any political subdivision thereof, but only to the extent of, and for the purposes set forth in, such order; provided, however, that Receiving Party shall first and immediately notify Disclosing Party in writing of the order and permit Disclosing Party to seek an appropriate protective order.

(5) ©Both parties further agree to exercise the same degree of care that it exercises to protect its own Confidential Information of a like nature from unauthorized disclosure, but in no event shall a less than reasonable degree of care be exercised by either party.

2. Designation.

(a) Information shall be deemed confidential and proprietary and subject to the restrictions of this Agreement if, when provided in:

(i) written or other tangible form, such Information is clearly marked as proprietary or confidential when disclosed to Receiving Party; or

(ii) oral or other intangible form, such Information is identified as confidential or proprietary at the time of disclosure.

3. Cooperation. Receiving Party will immediately give notice to Disclosing Party of any unauthorized use or disclosure of the Information of Disclosing Party.

4. Ownership of Information. All Information remains the property of Disclosing Party and no license or other rights to such Information is granted or implied hereby. Notwithstanding the foregoing, Disclosing Party understands that Receiving Party may currently or in the future be developing information internally, or receiving information from other parties that may be similar to Information of the Disclosing Party. Notwithstanding anything to the contrary, nothing in this Agreement will be construed as a representation or inference that Receiving Party will not develop products, or have products developed for it, that, without violation of this Agreement, compete with the products or systems contemplated by Disclosing Party's Information.

5. No Obligation. Neither this Agreement nor the disclosure or receipt of Information hereunder shall be construed as creating any obligation of a Party to furnish Information to the other Party or to enter into any agreement, venture or relationship with the other Party.

6. Return or Destruction of Information.

(a) All Information shall remain the sole property of Disclosing Party and all materials containing any such Information (including all copies made by Receiving Party) and its Representatives shall be returned or destroyed by Receiving Party immediately upon the earlier of:

(i) termination of this Agreement;

(ii) expiration of this Agreement; or

(iii) Receiving Party's determination that it no longer has a need for such Information.

(b) Upon request of Disclosing Party, Receiving Party shall certify in writing that all Information received by Receiving Party (including all copies thereof) and all materials containing such Information (including all copies thereof) have been destroyed.

7. **Injunctive Relief**: Without prejudice to any other rights or remedies that a party may have, each party acknowledges and agrees that damages alone may not be an adequate remedy for any breach of this Agreement, and that a party shall be entitled to seek the remedies of injunction, specific performance and/or any other equitable relief for any threatened or actual breach of this Agreement

8. Notice.

(a) Any notice required or permitted by this Agreement shall be in writing and shall be delivered as follows, with notice deemed given as indicated:

(i) by personal delivery, when delivered personally;

(ii) by overnight courier, upon written verification of receipt; or

(iii) by certified or registered mail with return receipt requested, upon verification of receipt.

(b) Notice shall be sent to the following addresses or such other address as either Party specifies in writing.

RailTel Corporation of India limited:

Attn: _____
Address:_____
Phone:
Email.

_____**:**

Attn:
Address:
Phone:
Email:

9. Term, Termination and Survivability.

(a) Unless terminated earlier in accordance with the provisions of this agreement, this Agreement shall be in full force and effect for a period of _____ years from the effective date hereof**.**

(b) Each party reserves the right in its sole and absolute discretion to terminate this Agreement by giving the other party not less than 30 days' written notice of such termination.

(c) Notwithstanding the foregoing clause 9(a) and 9 (b) , Receiving Party agrees that its obligations, shall:

(i) In respect to Information provided to it during the Term of this agreement, shall survive and continue even after the expiry of the term or termination of this agreement; and

(ii) not apply to any materials or information disclosed to it thereafter.

10. Governing Law and Jurisdiction. This Agreement shall be governed in all respects solely and exclusively by the laws of India without regard to its conflicts of law principles. The Parties hereto expressly consent and submit themselves to the jurisdiction of the courts of New Delhi.

11. Counterparts. This agreement is executed in duplicate, each of which shall be deemed to be the original and both when taken together shall be deemed to form a single agreement

12. No Definitive Transaction. The Parties hereto understand and agree that no contract or agreement with respect to any aspect of a potential transaction between the Parties shall be deemed to exist unless and until a definitive written agreement providing for such aspect of the transaction has been executed by a duly authorized representative of each Party and duly delivered to the other Party (a "***Final Agreement***"), and the Parties hereby waive, in advance, any claims in connection with a possible transaction unless and until the Parties have entered into a Final Agreement.

13. Settlement of Disputes:

a) The parties shall, at the first instance, attempt to resolve through good faith negotiation and consultation, any difference, conflict or question arising between the parties hereto relating to or concerning or arising out of or in connection with this agreement, and such negotiation or consultation shall begin promptly after a Party has delivered to another Party a written request for such consultation.
b) In the event of any dispute, difference, conflict or question arising between the parties hereto, relating to or concerning or arising out of or in connection with this agreement, is not settled through good faith negotiation or consultation, the same shall be referred to arbitration by a sole arbitrator.
c) The sole arbitrator shall be appointed by CMD/RailTel out of the panel of independent arbitrators maintained by RailTel, having expertise in their respective domains. The seat and the venue of arbitration shall be New Delhi. The arbitration proceedings shall be in accordance with the provision of the Arbitration and Conciliation Act 1996 and any other statutory amendments or modifications thereof. The decision of arbitrator shall be final and binding on both parties. The arbitration proceedings shall be conducted in English Language. The fees and cost of arbitration shall be borne equally between the parties.

14. CONFIDENTIALITY OF NEGOTIATIONS

Without the Disclosing Party's prior written consent, the Receiving Party shall not disclose to any Person who is not a Representative of the Receiving Party the fact that Confidential Information has been made available to the Receiving Party or that it has inspected any portion of the Confidential Information or that discussions between the Parties may be taking place.

15. **REPRESENTATION**

The Receiving Party acknowledges that the Disclosing Party makes no representation or warranty as to the accuracy or completeness of any of the Confidential Information furnished by or on its behalf. Nothing in this clause operates to limit or exclude any liability for fraudulent misrepresentation.

16. ASSIGNMENT

Neither this Agreement nor any of the rights, interests or obligations under this Agreement 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 Agreement will be binding upon, inure to the benefit of, and be enforceable by, the Parties and their respective successors and assigns.

17. EMPLOYEES AND OTHERS

Each Party shall advise its Representatives, contractors, subcontractors and licensees, and shall require its Affiliates to advise their Representatives, contractors, subcontractors and licensees, of the obligations of confidentiality and non-use under this Agreement, and shall be responsible for ensuring compliance by its and its Affiliates' Representatives, contractors, subcontractors and licensees with such obligations. In addition, each Party shall require all persons and entities who are not employees of a Party and who are provided access to the Confidential Information, to execute confidentiality or non-disclosure
agreements containing provisions no less stringent than those set forth in this Agreement. Each Party shall promptly notify the other Party in writing upon learning of any unauthorized disclosure or use of the Confidential Information by such persons or entities.

18. NO LICENSE

Nothing in this Agreement is intended to grant any rights to under any patent, copyright, or other intellectual property right of the Disclosing Party, nor will this Agreement grant
the Receiving Party any rights in or to the Confidential Information of the Disclosing Party, except as expressly set forth in this Agreement.

19. RELATIONSHIP BETWEEN PARTIES:

Nothing in this Agreement or in any matter or any arrangement contemplated by it is intended to constitute a partnership, association, joint venture, fiduciary relationship or other cooperative entity between the parties for any purpose whatsoever. Neither party has any power or authority to bind the other party or impose any obligations on it and neither party shall purport to do so or hold itself out as capable of doing so.

20: **UNPULISHED PRICE SENSITIVE INFORMATION (UPSI)**

_____ agrees and acknowledges that _____, its Partners, employees, representatives etc., by virtue of being associated with RailTel and being in frequent communication with RailTel and its employees, shall be deemed to be "Connected Persons" within the meaning of SEBI (Prohibition of Insider Trading) Regulations, 2015 and shall be bound by the said regulations while dealing with any confidential and/ or price sensitive information of RailTel. _____ shall always and at all times comply with the obligations and restrictions contained in the said regulations. In terms of the said regulations, _____ shall abide by the restriction on communication, providing or allowing access to any Unpublished Price Sensitive Information (UPSI) relating to RailTel as well as restriction on trading of its stock while holding such Unpublished Price Sensitive Information relating to RailTel.

21 MISCELLANEOUS. This Agreement constitutes the entire understanding among the Parties as to the Information and supersedes all prior discussions between them relating thereto. No amendment or modification of this Agreement shall be valid or binding on the Parties unless made in writing and signed on behalf of each Party by its authorized representative. The failure or delay of any Party to enforce at any time any provision of this Agreement shall not constitute a waiver of such Party's right thereafter to enforce each and every provision of this Agreement. In the event that any of the terms, conditions or provisions of this Agreement are held to be illegal, unenforceable or invalid by any court of competent jurisdiction, the remaining terms, conditions or provisions hereof shall remain in full force and effect. The rights, remedies and obligations set forth herein are in addition to, and not in substitution of, any rights, remedies or obligations which may be granted or imposed under law or in equity.

IN WITNESS WHEREOF, the Parties have executed this Agreement on the date set forth above.

_____:	**RailTel Corporation of India Limited:**
By_____	By_____
Name:	Name:
Title:	Title:

Witnesses

Annexure-6: EMD (as PBG) Format

BG NO :
ISSUANCE DATE : DD-MM-YYYY
BG AMOUNT : Rs xxxxxxx /-
EXPIRY DATE : DD-MM-YYYY
CLAIM EXPIRY DATE : DD-MM-YYYY

In consideration of the **RailTel Corporation of India Limited, (**CIN: L64202DL2000GOI107905**)** having its registered office at Plate-A, 6th Floor, Office Block Tower-2, East Kidwai Nagar, New Delhi – 110023 (Here in after called RailTel) having agreed to exempt ~~**Partner Name (CIN:)**~~ having its registered office at ~~**Partner's address**~~ (Here in after called "the said Contractor(s)") from the demand, under the terms and conditions of **EOI NO.** made between **RailTel Corporation of India Limited** and ~~**Partner Name**~~ for (here in after called "the said Agreement") of security deposit for the due fulfilment by the said contractor (s) of the terms and conditions contained in the said Agreement, or production of a Bank Guarantee for **Rs. /- (In Words).**

We, ~~**Bank Name**~~ a banking company incorporated under the Companies Act, 1956 and carrying on Banking Business under The Banking Regulation Act, 1949 and having its Registered Office at ~~**Bank's Address**~~ and its Central office at ~~**Bank's Corporate Office Address**~~ (indicate the name of the Bank) here in after referred to as "the Bank") at the request of ~~**Partner's Name**~~ Contractor(s) do hereby undertake to pay the **RailTel** an amount not exceeding ~~**Rs /- (In Words)**~~ .. 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 said Contractor(s) of any of the terms or conditions contained in the said Agreement.

We, ~~**Bank Name**~~ do here by undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the **RailTel** stating that the amount as 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 terms and conditions contained in the said Agreement or by 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. /- (In Words).**

We, ~~**Bank's Name**~~ undertake to pay to the **RailTel** any money so demanded not with standing any dispute or disputes raised by the Contractor(s) / Supplier(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)/ Supplier(s) shall have no claim against us for making such payment.

We, ~~**Bank's Name**~~ further agree that the Guarantee here in 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 discharge this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the **DD-MM-YYYY(Claim Expiry Date.)** We shall be discharged from all liability under this Guarantee thereafter.

We, ~~**Bank's Name**~~ 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 or 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 effect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the bank or the Contractor(s) Supplier(s).

~~**Bank's Name**~~ lastly undertake not to revoke this Guarantee during its currency except with the previous consent of the **RailTel** in writing.

Date : DD-MM-YYYY
Place :

Annexure-7: Non-Disclosure Undertaking (NDU) Format

NON DISCLOSURE UNDERTAKING

To,

RailTel Corporation of India Limited

Plate-A, 6th Floor, Office Block Tower-2,

East Kidwai Nagar, New Delhi-110023

(Hereinafter referred to as "RailTel" or "Disclosing Party" "Tender Floating Agency")

We, _____(CIN:____), a company duly incorporated under the Companies Act, 1956 and having its registered office at _____ (hereinafter referred to as the "Bidder/Receiving Party", which expression shall, unless repugnant to or inconsistent with the context or meaning thereof mean and include its successors and permitted assigns), do hereby solemnly declare and state as follows:-

1. We are the Bidders/Prospective Bidders for the EOI floated by RailTel for Implementation of Supply, installation, configuration, commissioning & integration of ICT infrastructure for End Customer Data Centre along with it's operation and maintenance.

2. We are well aware that the said tender relates to for procurement of services and equipment for high security installations. Hence, being a prospective bidder, we agree and acknowledge that it becomes imperative on our part to maintain utmost confidentiality in relation to said tender.

3. We undertake that any information relating to said tender (hereinafter referred to as the Confidential Information) which is or will be disclosed/ divulged by RailTel as a Disclosing Party to us, will be received and treated by us as strictly confidential and we shall not, without the prior written consent of the RailTel or as expressly permitted herein, disclose or make available to any other person such information.

4. We agree and undertake that we shall use any such information relating to said tender only for the purpose of bidding in the tender and will not use for any other purpose whatsoever.

5. We further undertake that we will disclose such Confidential Information to our employees or Representatives only on a strict "need to know" basis, for the sole purpose of preparation and submission of our Bid subject to such employee or representative being bound by the confidentiality obligation hereunder. We shall be responsible for any breach of the terms of this Undertaking by us or by any of our employees or Representatives.

6. We undertake that we shall exercise no lesser security or degree of care than we apply to our own Confidential Information of an equivalent nature, but in any event not less than the degree of care which a reasonable person with knowledge of the confidential nature of the information would exercise.

7. We shall ensure that all such Confidential Information is kept safe and secured at all times and is protected from unauthorized access, use, dissemination, copying, theft or leakage.

8. We undertake that we shall at no time, discuss with any person, other than as permitted under this Undertaking, the Confidential Information, or any other matter in connection with, or arising out of, the discussions or negotiations in relation to the Bid Process.

9. Without prejudice to any other rights or remedies that RailTel may have, we agree and acknowledge that in the event of a breach or threatened breach of the provisions of this Undertaking, money or damages may not be an adequate remedy for a breach of any of the provisions of this

Undertaking and it is reasonable that the RailTel, in addition to any other relief or remedy that it may have, shall also be entitled to the injunctive relief, specific performance and other equitable relief for any threatened or actual breach of the provisions of this Undertaking.

10. In case any loss or damages are incurred by RailTel owing to any breach or threatened breach by us, we undertake to hold RailTel harmless and indemnify in full to RailTel for any such loss.

11. We hereby represents and warrants that we have the requisite power and authority to execute, deliver and perform its obligations under this Undertaking.

12. The terms and conditions of this Undertaking shall inure to the benefit of and be binding upon the successors and permitted assigns of the Parties. The obligations under this Undertaking shall not be assigned or otherwise transferred in whole or in part by either party without the prior written consent of the other parties.

13. The obligation relating to confidentiality under this undertaking shall survive even after award of the project and successful completion of project.

For and on behalf of

Authorized Signatory
Name
Designation

Appendix (A)

**********Tender document of Customer of RailTel (CoR)**********

NATIONAL INFORMATICS CENTRE SERVICES INC.(NICSI)

(A Government of India Enterprise under NIC)

Ministry of Electronics & Information Technology (MeitY)

Government of India

(Estimated Tender Value: INR 60 Cr.)

ICT Enablement for Supreme Court of India Data Centre

Corrigendum to Bid no: GEM/2024/B/4564249

1st FLOOR, NBCC TOWER

15, BHIKAJI CAMA PLACE, NEW DELHI – 110066

TEL – 22900525, 534/35, FAX – 26105212

DISCLAIMER & DISCLOSURES

This Request for Proposal ("RFP / Tender/ Bid Document") is issued by National Informatics Centre Services Inc. (NICSI).

A. The information contained in this RFP/Bid Document or information provided subsequently to bidder(s) or vendor(s) whether verbally or in documentary form by or on behalf of NICSI, is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

B. Whilst the information in this RFP has been prepared in good faith, it is not and does not purport to be comprehensive or to have been independently verified. The information is not intended to be exhaustive. Interested parties are required to make their own inquiries and bidders will be required to confirm that they have done so and they do not rely only on the information provided by NICSI in submitting response to the RFP document. The information is provided on the basis that it is non–binding on NICSI or any of its authorities, agencies, officers, employees, agents, or advisors. NICSI reserves the right not to proceed with the Project or to change the configuration of the Project, to alter the timetable reflected in this document or to change the process or procedure to be applied. No reimbursement of cost of any type will be paid to persons or entities participating in the process.

C. Scope of Work (SoW) specified herein or makes any representation or warranty, express or implied, with respect to the information contained in this RFP or on which this RFP is based or with respect to any written or oral information made or to be made available to any of the recipients or their professional advisers and, so far as permitted by law and except in the case of fraudulent misrepresentation by the party concerned, and liability therefore is hereby expressly disclaimed.

D. Any product name / function used in this document are meant to be generic and do not refer to the product of any particular company/OEM/Vendor . In case such proprietary terms have been inadvertently mentioned then such terms should be taken to refer to the generic technology(ies). Bidders with industry standard equivalent product name / function under any other name will also be eligible to submit their bids.

E. This RFP document is not an agreement and is neither an offer. The purpose of this RFP is to provide applicants who are shortlisted to submit the bids ("Bidders") with information to assist them in formulation of their proposals ("Bids"). This RFP does not claim to contain all the information each bidder may require. Each bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability, and completeness of the information in this RFP. NICSI makes no representation or warranty, express or implied, and shall incur no liability whatsoever under any law, statute, rules, or regulations as to the accuracy, reliability or completeness of this RFP. NICSI may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

F. The information contained in this RFP is selective and is subject to updating, expansion, revision, and amendment at the sole discretion of NICSI. It does not, and does not purport to, contain all the information that a recipient may require for the purposes for deciding for participation in this process.

G. NICSI reserves the right to reject any or all the responses to this RFP at any stage without assigning any reason whatsoever and without being liable for any loss/injury that bidder might suffer due to such rejection. The decision of Supreme Court of India /NICSI shall be final, conclusive, and binding to all the parties directly or indirectly connected with the bidding process.

H. It may be noted that notice regarding corrigenda, addendums, amendments, time-extensions, clarifications, response to bidders' queries etc., if any to RFP, will not be published through any advertisement in newspapers or any other media.

Table of Contents

1 Objective of the RFP

Supreme Court of India is intended to build Data Centre at Supreme Court, New Delhi premises for hosting their secured Intranet applications and related services along with other mission critical applications.

The proposed data centre will consist of 20 racks with all latest technologies inbuilt. In addition to Data center, a command control center which will also be built where 24X7 monitoring will be done for Network, storage and compute infrastructure and all critical applications.

Through this RFP, a Managed Service Provider (MSP) shall be selected to supply, install, configuration, test and commission various ICT components required at the data centre along with 5 years of onsite comprehensive warranty & support as per Annexure: Un-priced BOQ. The MSP shall also provide operation and maintenance services for the deployed ICT infrastructure for a period of 5 years from the date of acceptance of the solution by deploying required technical manpower.

2 Scope of Work

The overall scope of work of the RFP can be divided into 2 parts viz.

1. Supply, installation, configuration, commissioning & integration of ICT infrastructure.
2. Operation and Maintenance of the ICT infrastructure in compliance with the SLA as defined in Sr. No 5.

The brief scope of work of the RFP is defined below:

1. MSP shall install and commission the required IT hardware assets and software components into the racks at Supreme Court of India Data Centre, New Delhi.
2. The MSP shall centrally monitor and manage the devices & solutions on a 24x7x365 basis to ensure an uptime of 99.98% for all the ICT infrastructure**.**
3. MSP shall position a dedicated technical onsite team to implement, commission and manage the ICT infrastructure deployed in in accordance with the necessary security policies and issued guidelines by Supreme Court of India time to time.
4. The onsite team deployed by the MSP shall regularly monitor and troubleshoot the ICT infrastructure in compliance with the SLA as defined in Sr. No. 5
5. The MSP shall ensure that the Standard operating Procedures, policies and guidelines etc. for the data centre is fully compliant to the latest certification requirements of ISO 20000, ISO 27001, ISO 22301, ISO 27701, ISO 27017 etc. Supreme Court of India may hire an auditing agency through a separate process for conducting various audits. During the audit if that agency identifies any shortcoming/ lack of compliance, the MSP shall extend all kind of assistance in removing shortcoming/ lack of compliance in consultation with Supreme Court of India.
6. For detailed requirement specifications for each of the hardware and software components, please refer to Annexure: Technical Specification of the RFP

2.1 Supply, installation, Testing and Commissioning of ICT infrastructure.

A. The scope of work is to supply, installation, testing and commissioning of various ICT infrastructure components, provided as per the Annexure : Un-Priced BoQ along with warranty and support for 5 years.

B. In case any supporting accessories (Patch cords, hardware accessories, blanking panels etc.) and efforts, are required for running the overall solution which is not covered in the Annexure: Un-priced BoQ and the Scope of Work, the MSP shall provide the same to ensure smooth operations of the overall solution at no additional cost to Supreme Court of India/ NICSI.

C. All required patch cords (copper and fiber) for the overall commissioning of the solution have to be provided by the MSP.

D. Structured cabling/Connectivity of inter rack and intra rack with necessary redundancy will be performed by the MSP, if the MSP deems it necessary.

E. The MSP will set up all the virtual solutions procured through this RFP on the servers procured through this RFP and it should not be any external cloud based solution. The MSP shall provision all the software, licenses and other components required for the overall commissioning of the solution and also ensure the availability of solutions as per Sr. No 5 SLA.

F. To meet the SLA requirements, the MSP shall enhance the capacity of all required resources in the event of unsatisfactory performance of infrastructure/services.

G. None of the solutions/ items supplied by the MSP should become End- of-life or End-of-support during the contract period. In case any of the solutions /devices becomes EOL or EOS during the contract period, then the MSP will have to replace the solution/devices with equal or higher specification with due approval of Supreme Court of India/ /NICSI.

H. Entire solution (hardware & software) should be IPv6 implementation ready from day one, considering IPv6 security practices.

I. The MSP shall ensure the entire architecture of the overall solution is able to sustain failure of minimum two nodes.

J. The MSP shall supply, install, commission and test open source database solutions.

K. Supreme Court of India/NICSI may conduct third party audit on the infrastructure as per need. The MSP shall have to implement all such audit recommendations on priority, under the supervision of Supreme Court of India/NICSI.

L. All the ICT infrastructure including hardware and software items will be under the ownership of Supreme Court of India. All software licenses/ subscriptions deployed by the MSP should be of enterprise class only.

M. The MSP should provide comprehensive onsite warranty on a 24 x 7 x 365 basis for a period of 5 (Five) years from the date of acceptance on all ICT infrastructure solution provided as part of scope of work. The warranty period shall commence from the date of Final acceptance (FAT) of the entire solution/system as described in RFP.

2.2 Operation and Maintenance of the ICT infrastructure

A. The MSP shall be responsible for the overall Operations and Maintenance of the ICT infrastructure which covers all the ICT equipment as well as managing and maintaining the cloud operation on a 24X7 basis as per the defined SLA in Sr. No. 5, including but not limited to following:

2.2.1 Management of Data Centre Infrastructure

A. The MSP shall be responsible for the management of entire cloud and ICT landscape of the Data Centre such as compute, storage, backup, virtualization & cloud, network, security etc.

B. The MSP shall centrally monitor and manage the devices & solutions on a 24x7x365 basis to ensure an uptime of 99.98% for the infrastructure as per SLA as defined in Sr. no 5 of the RFP.
C. The MSP shall be responsible for the Management reporting. The MSP shall maintain and use the required tools for periodic management reporting of key performance indicators in line with the SLA framework proposed. A separate access of the monitoring tools is to be provided to the Supreme Court of India /NICSI personnel.
D. Supreme Court of India /NICSI reserves rights to have control over operations delivered by MSP. Supreme Court of India/NICSI can pitch in as a prominent decision maker in any crucial decisions made by MSP w.r.t architecting, solutioning, provisioning or any other cloud or infrastructure related activities pertaining to data centre.
E. The MSP should provide comprehensive technical support services for all the equipment installed for the entire period of the contract.
F. The MSP shall ensure that the data centre hygiene is maintained at all times including infrastructure migration. It will be a regular exercise done by the MSP throughout the O&M period.
G. The onsite support staff should possess capability for supporting the equipment and components proposed, but not limited to undertaking preventive and break-fix maintenance, troubleshooting, resolving problems, tuning, etc. The MSP shall also provision for necessary offsite support to ensure continuity of operations for Supreme Court of India/NICSI.
H. The MSP shall develop a mechanism that captures the packets from user to server within the datacentre (including all devices/ solution coming between user to application)
I. The MSP shall provide comprehensive technical support services for all the hardware and software proposed for the entire period of the contract. The technical support should include all the upgrades, updates and patches hot fixes, bug fixes that are released by the respective OEMs during the period of contract.

2.2.2 Managed Cloud and IT infrastructure Services

A. MSP shall perform operation and maintenance of the IT infrastructure including onsite service desk and 24x7x365 operations from the Data centre.
B. The Managed services to be performed by the MSP will include but not limited to:
    1. Managed compute services.
    2. Managed storage services.
    3. Directory services / AD / LDAP services and all related services like DNS, DHCP etc.
    4. Managed database services.
    5. Managed backup services along with offsite backup operation (tapes) and conduct a backup verification and testing exercises on quarterly basis.
    6. Compliance to prevalent data localization laws and guideline issued by Govt. of India and other regulatory bodies/authorities to be strictly adhere too. Necessary actions/solutions framework to be put in place by MSP to ensure compliance.
    7. Application/software/OS which includes MS-Window, Linux-Red Hat etc. license and support management.
    8. Configuration and management of endpoints (imaging, deployment, driver, and patching updates, etc.)

9. Asset and inventory management.
10. Managed network services by coordinating with connectivity provider.
11. Support of all services including incident, configuration, change and problem management, etc.
12. MSP shall provide the necessary updates, upgrades and security fixes for all IT infrastructure components and tools deployed at the Data Centre during the lifecycle of the contract.
13. MSP shall perform maintenance and development of Local Area Network at the Sites
14. MSP will prepare SOPs for all activity to done by any device /solution/approval process etc.
15. MSP will maintain register for Realtime resource utilisations of all servers/devices etc.
16. MSP shall provide all requisite documentation, including periodic updates.
17. Necessary network and security Layer including Hardware and Software requirement necessary to enforce security and data throughput should be put by MSP to ensure the required SLA defined at Sr.no 5. Necessary access rights, visibility, control, and access logs will be provided to Supreme Court of India.

2.2.3 Onsite support

A. The MSP should ensure that the entire ICT Infrastructure solution is operational in accordance with the stipulated service standards as per the SLA as defined in Sr.No 5 .

1. The bidder along with all the associated OEMs should commit to provide all necessary resources and expertise to resolve any issues and carry out required changes, optimizations and modification to ensure that the ICT infrastructure is operational.
2. The onsite technical support should also include all the upgrades, updates and patches that are released by the respective OEMs during the period of contract.

2.2.4 Technical Support

A. The onsite technical team will coordinate with Supreme Court of India/NICSI for the resolution of all ICT infrastructure related issues / problems. The Technical Support desk shall undertake the following activities:
   1. Log issues / complaints related to ICT infrastructure at the Data Centre and issue an ID number against the issue / complaint.
   2. Assign severity level to each issue / complaint so as to maintain categorization and differentiate the criticality of the incident via the priority levels, severity levels and impact levels.
   3. Track each issue / complaint to resolution.
   4. Escalate the issues / complaints, to Supreme Court of India /NICSI officials, if necessary, as per the escalation matrix defined in discussion with Supreme Court of India /NICSI.
   5. Analyse the issue / complaint statistics and bidder's SLA.
   6. Should provision for all necessary channels for reporting issues to onsite technical team. The incident reporting channels will be the following:
      i. Email
      ii. Telephone (mobile phone alerts)
      iii. Web Based

B. The onsite technical support team shall troubleshoot and will provide Root Cause Analysis (RCA) for any outage/ data breach/ incident of any application/ device/ solution/ data centre.

2.2.5 System Maintenance and Management

A. Certain minimum deliverables sought from the MSP with regards to System Maintenance and Management are provided below: -

1. The MSP shall be responsible for tasks including but not limited to setting up servers, configuring and apportioning storage space, account management, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary.
2. The MSP shall provision skilled and experienced manpower resources to administer and manage the entire ICT Infrastructure solution at the Data Centre.
3. On an ongoing basis, the MSP shall be responsible for troubleshooting issues in the ICT infrastructure solution to determine the areas where fixes are required and ensuring resolution of the same.
4. The MSP shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the ICT Infrastructure and maintaining the defined SLA at Sr. No 5.
5. The MSP shall be responsible for managing the usernames, roles and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc.
6. The MSP shall be responsible for management of passwords for all relevant components and devices under his purview and implement a password change mechanism in accordance with the security policy and guidelines formulated in discussion with Supreme Court of India and based on the industry best practices & frameworks like ISO 27001, ISO 20000, ISO 22301 etc.
7. MSP shall be responsible for shutting down the VMs/Servers/cloud accounts of management infrastructure which are not used for a long time.

2.2.6 System Administration

A. Certain minimum deliverables sought from the MSP with regards to System Administration are provided below:-

1. The MSP shall ensure proper configuration of server parameters. The bidder shall be the single point of accountability for all the hardware maintenance and support for the ICT infrastructure at the Data Centre.
2. The MSP shall be responsible for Operating system administration, including but not limited to management of users, processes, preventive maintenance and management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.
3. The MSP shall also be responsible for installation and re-installation in the event of system crash/failures.
4. The MSP shall appoint system administrators to regularly monitor and maintain a log of the monitored servers to ensure their availability to Supreme Court of India at all times.
5. The MSP shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall undertake actions in accordance with the results of the log

analysis. The system administrators should also ensure that the logs are backed up and truncated at regular intervals. The MSP are advised to refer CERT-In Guidelines so as to ensure their alignment with the practices followed.

6. The system administrators should adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system, applying patches, etc.
7. The system administrators should provide hardening of servers in line with the defined security policies & guidelines of Supreme Court of India as well as based on industry best practices.
8. The system administrators should provide integration and user support on all supported servers, data storage systems etc.
9. The system administrators should provide directory services such as local LDAP services and DNS services, NTP services and user support on all supported servers, data storage systems etc. The system administrators will be required to trouble shoot problems with web services, application software, desktop/server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.
10. The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in *Service Level Agreement.*

2.2.7 Storage Administration

A. Certain minimum deliverables sought from the MSP with regards to Storage Administration are provided below:-

1. The MSP shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN fabric / switches, Virtual tape library, storage servers etc.
2. The MSP shall be responsible for storage management, including but not limited to management of space, SAN volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.
3. Supreme Court of India/NICSI would additionally remotely manage the storage system and components and appropriate setup should be provided by the MSP
4. The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.
5. The storage administrator will be required to create/delete, enable/disable zones in the storage solution.
6. The storage administrator will be required to create / delete / modify storage volumes in the storage solution.
7. The storage administrator will be required to create / delete, enable / disable connectivity and access rights to storage volumes in the storage solution.
8. To facilitate scalability of solution wherever required.

2.2.8 Database Administration

A. The MSP shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.

1. The MSP shall be responsible to perform physical administrative functions such as reorganizing the database to improve performance.
2. The MSP shall be responsible for tuning of the relational database, ensuring the integrity of the data and configuring the data dictionary.
3. The MSP shall be responsible for testing and installing new database software releases, if any.

2.2.9 Backup / Restore

A. The MSP shall be responsible for backup of storage as per the policies and guidelines of Supreme Court of India/NICSI at the Data Centre. These policies would be discussed with the MSP at the time of installation and configuration.

1. The MSP shall be responsible for monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups and ensuring adherence to retention policies of Supreme Court of India.
2. The MSP shall be responsible for prompt execution of on-demand backups of volumes and files whenever required or in case of upgrades and configuration changes to the system.
3. The MSP shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. The MSP shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.
4. The administrators shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fireproof cabinets (onsite and offsite).
5. The MSP shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre.

2.2.10 Network Operations

A. The MSP shall provide services for management of network environment to maintain performance at optimum levels on a 24x7 basis. The MSP shall be responsible for monitoring and administering the network within the Data Centre up to the integration points with WAN. The MSP will be required to provide network related services for routers, switches, load balancer services etc.

B. The MSP shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic. The MSP shall co-ordinate with the basic infra service provider or any other third-party MSP of Supreme Court of India in case of break fix maintenance of the LAN cabling or maintenance work requiring civil work.

2.2.11 Command and Control Centre (CCC)

A. As part of this RFP, the MSP shall set up an onsite Command and Control Centre (CCC) for managing and monitoring the complete Cloud and ICT infrastructure of the data centre such as Compute, Storage, Switches, Routers, Firewalls, security infrastructure, Databases, applications (but not limited to) as part of the project. The MSP shall provide management & monitoring services through implementation of respective tools and technologies and shall provide qualified manpower for 24x7 operations. The CCC provides the following operational services:

- **Security Operations:** Monitor the system logs, and security events to identify suspicious or malicious activities. Monitoring security patches and updates. Observe access logs related to access control at OS & DB.
- **Cloud Ops:** Monitoring of cloud resources and services to detect performance issues and security threats.
- **Infrastructure Operations:** Monitor the health, performance and availability of infrastructure components such as servers, storage and networking equipment.
- **Network Operations:** Monitor the network infrastructure to identify issues and potential security threats. Network Ops teams to track network health and status.
- **Database Operations:** Monitor the health, performance, and availability of databases. Detect issues, such as performance bottlenecks and potential security threats.
- **Middleware Operations:** Observe the performance, availability and health of middleware components. Respond to issues, performance bottlenecks and resource constraints.

2.2.12 Information Security Monitoring and Management

A. The MSP shall provide monitoring and management services for the provisioned infrastructure systems related to information security. Management of this environment in order to ensure confidentiality, integrity, availability and non-repudiation of the services on a 24x7 basis. The team will be required to provide monitoring and management of activities including but not limited to the following:-

2.2.12.1 Firewall Monitoring and Management

a. Installation and maintenance of the firewall
b. Firewall hardening with initial configuration.
c. Performance monitoring
d. Regular monitoring of the LAN errors
e. Regular monitoring of utilisation of CPU, memory of Data Plane and Control Plane.
f. Firewall rule-based policy creation, implementation and changes
g. Security Policy Configuration
h. Create and maintain Network Access Policy (NAP) document (the access specification) agreed between the parties from time to time.
i. Log File review and analysis of information on traffic flow
j. Log File trend upgrade and analysis
k. Compliance Testing
l. Design, configure and maintain all Network Address Translation (NAT) services.
m. Access control management through creation of the Network Access Policy and firewall rules
n. Implementation and maintenance.
o. Manage access to F/W logs policies and performance statistics for viewing through secure web portals in conjunction with monitoring tools.
p. Manage the functioning of Regular Reports in conjunction with monitoring tools so as to provide detailed auditing of configuration history and change of journals. Alerts include critical configuration changes, potential malicious activity and operational alarms.
q. Incident response

r. Lifecycle Management of all Hardware and Software components
s. Firewall Backup

2.2.12.2 Network Based Intrusion Prevention System - Monitoring and Management

a. Traffic Profiling
b. Define Alert levels and Incident response levels.
c. Root cause analysis
d. Technical support
e. Monitor NIPS for 24*7 availability.
f. Restore NIPS availability.
g. Determine Intrusion occurrence.
h. Regularly Upgradation and updation of intrusion signatures
i. Testing and Verification of triggered signatures for false positive with OEMS.
j. Fine tuning of NIPS signatures,
k. Putting signatures in block mode at all NIPS.
l. Creation of user defined signatures as and when required by NICSI
m. Provide security event correlation.
n. Regular Monitoring of the attack logging rule's logs
o. Regular Monitoring of the generic deny rule's logs.
p. Regular Monitoring of the attack bandwidth utilization
q. Network attacks and serious attacks attempts analysis.
r. Assessment of uncovered new vulnerabilities.
s. Propose corrective and preventive actions.
t. Monitoring and subscribing to external network security information in order to evaluate new attacks and propose preventive steps.
u. Installation and configuration of NIPS Software and Hardware
v. Provide maintenance and upgrade of service component Software.
w. Provide reporting of intrusions and actions, web-based access
x. Regular Reports
y. Incidence response
z. Prevent all known network-based attacks.
aa. Filter out IP and TCP illegal packet types
bb. Designing and configuring IPS services in response to Flooding limits (per source, destination and intensity)
cc. Technical Support desk Support
dd. Lifecycle Management of all Hardware and Software components and 24*7 Real time Monitoring and Response.

2.2.12.3 Patch Management

A. The MSP will be required to provide services related to Patch Management. The security administrators should be aware of security precautions in place in their environment. Ensure that there is available documentation as to what traffic is being allowed through to the internal network. This will help in the evaluation of threats posed by known vulnerabilities and assign a risk factor to them. Personnel designated to evaluate patch stability should have expertise in mission critical systems and be capable of verifying stability of systems after patch installation.
B. Before any patch is installed, a full backup of all data and server configuration information must be made. Best practices for disaster recovery recommend periodic testing of the restore process to ensure the integrity of the backed-up data. The patch

management should be executed efficiently for all kinds of environments like for operating systems and Databases.

C. The activities mentioned above are indicative in nature. The MSP will be required to provide services related to Patch management as per Supreme Court of India Security Policies & guideline as well as future addendums.

2.2.12.4 Vulnerability Assessment (Quarterly)

A. This section provides an outline of the various items to be investigated during our Vulnerability Assessment phase. The said activities should follow the various guidelines for cyber security like Supreme Court of India and Cert-In Guidelines. The activities performed should be included but not limited to the following:

B. Vulnerability Assessment will scan for the following core areas:

1. Application based vulnerability assessment:
    a. To provide proper evaluation of security vulnerabilities associated with applications – any application installed at server like acrobat reader,.Net framework, Apache, IIS, Tomcat, thereby, recommend solutions to problems.
2. OS level vulnerability assessment:
    a. To provide proper evaluation of security vulnerabilities associated with operating systems – Unix, Linux, Sun OS, Windows, Mac OS etc. and recommend solutions to various problems and issues.
3. Database Vulnerability assessment:
    a. To provide proper evaluation of security vulnerabilities associated with database –Microsoft SQL Server, Postgres and MySQL etc., and recommend solutions to various problems and issues.

C. Vulnerability Assessment will include checks like Port scan, unnecessary or vulnerable services, file permission, user access control, password protection, system vulnerability etc.

2.2.12.5 OS Hardening

A. OS Hardening will include activities but not limited to the removal of all non-essential tools, utilities, and services with other system administration by activating & configuring all appropriate security features. The entire scope of this service will differ on different Operating System basis. Most of the Windows and Linux based Operating Systems will include following activities in conjunction to CIS (Center for Internet Security) & Supreme Court of India OS hardening policies and guidelines:

1. Broad category:
    a. User Account Management
    b. Access Control Management
    c. Configuration and supporting processes.
    d. System logging and auditing.
    e. Network and environmental variables.
2. A preview on the activities associated with Broad categories:
    a. Identifying unused or unnecessary ports.
    b. Disable/Shut down/remove unused and unnecessary services and daemons.
    c. Removing rogue connections: wireless and dial-up.
    d. Setting up filters for malicious content for each OS.
3. Test Backup and restoring procedures:
    a. Account Policies: Password policy, Account lockout policy etc.

b. Local server Policies: Audit policies, User rights assignments, security options etc.
c. Event logs settings
d. System services
e. Registry settings
f. File & Folder permissions

2.2.12.6 Penetration Testing (Quarterly)

A. The Penetration Testing will include activities but not limited to the test should simulate activities in conjunction to Supreme Court of India cyber security and Cert-In policies & guidelines. These activities should identify specific exploitable vulnerabilities and expose potential entryways to vital or sensitive data. The results should clearly articulate security issues & recommendations and create a compelling event for the entire management team to support a security program. The MSP shall also ensure that the Patches/bug fixes released by OEM should be included in the golden image within 15 days from the date of patch/bug fixes release, and the VA assessment scoring of all the golden images should be above 90. If the score is <90 then golden image should be not allowed for any commissioning and deployment purposes for production and pre-production environment.

B. A complete project based approach should be followed that covers areas including but not limited to the following:

1. Network Security
2. Network Surveying
3. Port Scanning
4. System Identification
5. Services Identification
6. Vulnerability Research & Verification
7. Application Testing & Code Review
8. Router Testing
9. Firewall Testing
10. Intrusion Detection System Testing
11. Trusted Systems Testing
12. Password Cracking
13. Denial of Service Testing
14. Containment Measures Testing

2.2.12.7 Service Level Monitoring and Management

A. The proposed service management system should provide a detailed service dashboard view indicating the health of each application and IT infrastructure in the organization and the health of the services they rely on in compliance to the SLAs.

B. The system should have a customized dashboard as per Supreme Court of India's requirements to provide insights on key performance indicators and parameter as defined in the SLA at Sr. No 5.

C. The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users /applications with the services they rely on and related Service / Operational Level Agreements.

Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.

D. The Service Level Agreements (SLAs) definition facility must support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).

E. SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.

F. The system must provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition, the capability to exempt any service outage from impacting an SLA must be available.

2.2.12.8 Reporting

A. The reports supported must include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.

B. The system must provide a historical reporting facility that will allow for the generation of on-demand and scheduled reports of Service-related metrics with capabilities for customization of the report presentation.

C. The system should provide for defining service policies like Service Condition High \ Low Sensitivity, Port Status High \ Low Sensitivity should be provided out of the box.

D. The system should display option on Services, Customer, SLA's, SLA templates. The customer definition option should allow to associate a service or an SLA with a customer.

2.2.12.9 Performance – Monitoring

A. The proposed performance management system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for all ICT components.

2.2.13 Incident Management

2.2.13.1 General

A. MSP shall manage, Resolve and Close all Incidents in accordance with this section and the applicable Service Levels. MSP acknowledges and agrees that the primary objective of Incident management is to restore normal service operation as quickly as possible and communicate the resolution to Supreme Court of India and application owner. MSP shall use ITIL-compliant Incident management processes to manage service disruptions, with the objective of minimizing adverse impacts and delays to Customer and Service Users. MSP shall provide the open source ITSM tool as part of the overall solution without any additional cost.

B. MSP shall perform the following Incident management sub-processes:

1. Verification and identification of Incident
2. Incident logging, categorization, and prioritization
3. Conduct Incident diagnosis.
4. Investigate and diagnose Incident.
5. Manage critical Incident.
6. Resolution and recover.
7. Management review
8. Incident Closure

9. Logging of Incidents

C. MSP shall ensure that all Incidents are logged in the ITSM Tool, and Supreme Court of India /NICSI shall be given access, as required. Where an Incident has occurred, it shall be logged by Supreme Court of India or the onsite team in the Incident Log Entry using the ITSM Tool. If MSP itself becomes aware of an Incident prior to it being logged on the ITSM Tool, the MSP shall immediately log the Incident using the ITSM Tool.

D. The MSP shall also update Incident Log Entry with the following information/details within the designated Response Time. This information/ details, if not automatically included by the ITSM Tool, should include:

1. the Severity Level for the Incident as determined in accordance with requirements furnished in this section.
2. a unique Incident Log Entry number (each number to be applied sequentially).
3. the date and time the Incident Log Entry is made.
4. the person/organization creating the Incident Log Entry; and
5. to the extent that MSP is aware of the number of System Users who have been affected, an estimate (produced with all due care and diligence) of that number.

E. The point in time at which an Incident shall be deemed "logged" shall be the point at which the Incident is first assigned to the resolver as evidenced by the ITSM Tool. MSP shall:

1. monitor the ITSM Tool for notifications of Incidents.
2. within the Response Time shall notify NICSI/ Supreme Court of India and Application owner by using the ITSM tool / email or any other method regarding the Response of each Incident logged:
   a. if the Incident is one for which MSP is not responsible because the Incident has nothing to do with the proper performance of the solution or the O&M Services, the MSP shall notify Supreme Court of India/ application owner, that it is not responsible for the Incident with proper root cause analysis and documentary proofs.
   b. once an incident has been logged, managed, and resolved.
   c. promptly update the Incident Log Entry so that the following information is always up to date; and

F. MSP shall provide Supreme Court of India / application owner with

1. the information required on the incident.
2. details of MSP's Personnel who have been assigned to the Incident.
3. details of any communications with the Incident Manager in connection with the Incident.
4. any notes and comments regarding any mitigating circumstances regarding the Incident; and
5. MSP's planned actions for Resolving the Incident including details, where applicable, of the estimated time within which such Incident will be remedied.

G. MSP shall proactively progress all Incidents and track and escalate all related issues to the appropriate personnel of Supreme Court of India/ Application Owner. Once the Incident is Resolved and MSP shall include all the required information in the respective Incident Log Entry, Close the respective Incident Log Entry and detail the reason for such closure.

2.2.13.2 Managing, Investigating and Resolving Incidents

A. In respect of each Incident, MSP shall:

1. Shall assign a single point of contact and shall regularly update Supreme Court of India / Application Owner, via the ITSM tool, email or any other mode required, on the progress of the Resolution of the Incident
2. to the extent that MSP has, or is able to gain access to, data and information which is needed to understand the nature, magnitude, and impact of the Incident, MSP shall provide such information to Supreme Court of India / Application Owner as quickly as reasonably possible to allow for investigation, diagnosis, and resolution of the Incident in accordance with the Severity Levels
3. attend all meetings which are scheduled for the purpose of managing and resolving the Incident, whether such meetings are scheduled by MSP, Supreme Court of India / Application Owner
4. ensure that MSP Personnel shall work whatever hours are necessary to ensure that Resolution and Closure in respect of an Incident is achieved in accordance with the Service Levels.

2.2.13.3 Severity Level Definitions

A. Each Incident shall be allocated a Severity Level using the Severity Level Criteria. Such allocation to be made by the entity (i.e., Supreme Court of India / Application Owner) that created the Incident Log Entry. If the entity was not MSP and the allocation was not made at the time the Incident Log Entry was first created, then the MSP shall assign the severity level as per the severity defined in the section.

B. If two (2) or more reports of the same Incident are allocated different Severity Levels, the applicable Severity Level shall be the highest Severity Level so allocated.

C. Supreme Court of India / Application Owner may, acting reasonably, change the Severity Level allocated to any Incident at any time.

D. The MSP shall increase or (subject to the written approval of Customer) decrease the Severity Level allocated to an Incident as soon as it becomes aware of any facts or circumstances that make such an increase or decrease appropriate, under the approval of Supreme Court of India / Application Owner.

E. If the Severity Level of an Incident is increased then, for the purposes of calculating the Resolution Time, the Incident Log Entry shall be deemed to have been created at the time of the Severity Level increase.

F. If a Severity Level is assigned incorrectly (having regard to the information available at the time) then, for the purpose of calculating the Resolution Time for that Incident, the Incident Log Entry shall be deemed to have been created at the time it was originally created.

G. In relation to any Incident, Supreme Court of India / Application Owner may review the allocation of the Severity Level. If Supreme Court of India / Application Owner (having regard to the information available to MSP or Customer at the time) determines that MSP failed to properly increase the Severity Level allocated to the Incident, Supreme Court of India / Application Owner may retrospectively allocate a different Severity Level to the Incident and the new Severity Level shall be deemed to have applied as from the point of creation of the relevant Incident Log Entry.

H. Irrespective of whether MSP agrees with the allocation of the Severity Level or not, MSP will continue to treat the Incident in accordance with Severity Level allocated by Supreme Court of India / Application Owner.

I. The following Severity Level Criteria shall be used for the purpose of determining the Severity Level to be allocated to an Incident:

Severity Level	Definition
Severity Level 1	Showstoppers involving major failure in the system (DC and overall operations). There are no usable workarounds available to fix the problem. Fatal errors such as general protection fault, system hangs etc. Furthermore, testing cannot proceed until the error is fixed. These also include complete or partial service unavailability including the incorrect behaviour of the system, security incidents resulting in breach of security etc.
Severity Level 2	Users face severe restrictions in the system irrespective of the cause. Workarounds are time consuming. System behaviour is inconsistent. Furthermore, testing cannot proceed in the relevant areas until the error is fixed. These also include severely degraded system performance, repeat calls (same issue reported at least twice), demonstrates a viable turnaround etc.
Severity Level 3	Moderate restrictions in the system irrespective of the cause. There are convenient and readily available workarounds. Only a few users are affected. Minor errors are to be fixed, but testing can proceed with workaround solutions.

2.2.13.4 Resolution Times

A. The time taken for Resolution of each Incident shall be measured from the moment the Incident Log Entry is created in the ITSM Tool (or ought reasonably to have been created, in the case of any unreasonable delay on the part of MSP in doing so) until the moment of Resolution of such Incident.

B. Resolution shall involve MSP implementing either a Temporary Fix or a Permanent Fix, which shall be recorded by the ITSM Tool.

C. If MSP chooses to implement a Permanent Fix, then Resolution shall be deemed to have occurred when Supreme Court of India / Application Owner confirms that the relevant Incident has been adequately addressed and that the relevant element of the Solution (or the relevant Track) functions and performs in accordance with the Requirements, their applicable Specifications and any other relevant requirements of the Agreement and there is no longer any impact on Supreme Court of India / Application Owner.

D. If MSP wishes to achieve Resolution by way of the implementation of a Temporary Fix, it shall provide Supreme Court of India / Application Owner with details of the Temporary Fix for approval, such details to include the intended effect of the Temporary Fix once implemented. If Supreme Court of India / Application Owner approves the Temporary Fix, then MSP shall immediately apply the agreed Temporary Fix. The Incident shall be considered resolved when MSP confirms to the satisfaction of the Supreme Court of India / Application Owner (and such satisfaction is confirmed in writing by Supreme Court of India / NICSI/ Application Owner, such confirmation not to be unreasonably withheld) that the intended effect of the Temporary Fix has been achieved.

E. If, after MSP has provided the confirmation, the Incident reoccurs within five (5) hours of such confirmation being given, the Incident shall be deemed not to have been Resolved. Any time that elapses thereafter will be added to the lapsed time previously logged in respect of that lapsed Incident.

F. If an Incident has not been Resolved at the end of the applicable Measurement Period in which it has occurred, Supreme Court of India / Application Owner shall treat the

Incident as ongoing, in which case the Resolution Time shall be calculated as set out in section above, and Service Credits, where the relevant Service Level is not achieved, shall occur, or begin to occur (as the case may be) until the Incident is Resolved.

G. Any dispute as to whether an Incident has been Resolved (following implementation of a Temporary Fix or Permanent Fix) and/or as to the timing of such Resolution shall be referred to the Dispute Resolution Procedure.

2.2.13.5 Escalation

A. In respect of any Incidents, Supreme Court of India / Application Owner shall be entitled to notify members of MSP's senior management as follows:
   1. Supreme Court of India / Application Owner may notify MSP's senior management team if a Severity Level 1 or 2 Incident or Problem is not Resolved or Permanently Fixed, respectively in accordance with the applicable Service Level; and
   2. Customer may notify MSP's senior management team at any stage if MSP is not progressing the Resolution/Permanent Fix to Supreme Court of India / Application Owner's satisfaction.
   3. In addition to notifying any of the persons referred to in section above, Supreme Court of India / Application Owner shall be entitled to require the attendance of any such person(s) at a meeting with Supreme Court of India / Application Owner and/or such third parties as Supreme Court of India / Application Owner may require to attend, to discuss the Incident and the steps that are being taken by MSP to resolve it. Any such meeting shall be at a time and location that Supreme Court of India / Application Owner shall require.

2.2.14 Managed Cyber Security Services (Solution/ Devices)

A. MSP shall perform the Managed Cyber Security Services set out in this section including detailed Scope for Operations and Maintenance.

B. MSP shall provide managed cyber security operations from the Go-Live Milestone Date for the Term.

C. MSP shall ensure all the personal data is stored in compliance with Digital Personal Data Protection Act, 2023. The MSP shall also ensure that personal data is being encrypted at rest and in motion, or used in tokenised form, or obfuscated/masked; and the access privileges to the back-end data segment are limited to the minimum necessary set of authorised users and are protected with multi-factor authentication.

D. MSP shall be responsible for comprehensive security administration, management, and maintenance activities for both the cloud infrastructure.

E. The Managed Cyber Security Services to be performed by MSP will include but not limited to
   1. cyber security governance, compliance, and risk management.
   2. security administration and management services.
   3. administration and management of network security components.
   4. administration and management of network and endpoint advanced persistent threats detection and response and sandboxing.
   5. DNS security administration and management.
   6. web application firewall (WAF) security administration and management.
   7. web traffic and content scanning and analysis.

8. mobile device management including the associated system administration and management.
9. endpoint security administration and management.
10. data security and data privacy administration and management.
11. data leakage prevention administration, policy design, management and incident monitoring, analysis, and reporting.
12. database activity monitoring including administration and management activities.
13. secure configuration management and file integrity monitoring including administration and management activities.
14. user identity and access management.
15. network, users and events behaviour analytics and threats detection and response.
16. security incidents response and recovery management services.
17. digital forensic and security investigation services (to be provided as a service for security breaches and incidents).
18. vulnerability assessment and penetration testing services.

2.2.15 MIS Reports and deliverables

A. The MSP shall be required to submit the reports on a regular basis in a format decided by Supreme Court of India. The following is only an indicative list of MIS reports which should be in conjunction with the reporting features highlighted in the RFP.

1. Daily reports

a. Summary of issues / complaints logged at the technical support desk.
b. Summary of resolved unresolved and escalated issues / complaints.
c. Log of backup and restoration undertaken

2. Weekly Reports

a. Issues / complaints analysis report for virus calls, call trend, call history, etc.
b. Summary of systems rebooted.
c. Summary of issues / complaints logged with the OEMs.
d. Inventory of spare parts in the Data Centre
e. Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

3. Monthly Reports

a. Component wise ICT infrastructure availability and resource utilization
b. Adherence report as per the SLA as defined in Sr. No 6.
c. Summary of changes in the Data Centre
d. Log of preventive / scheduled/ break-fix maintenance undertaken.
e. Summary of attendance of MSP's staff at the Data Centre

4. Quarterly Reports

a. Adherence report to the SLA as defined in Sr. No 6 and resource utilization

2.2.16 OEM's Responsibilities

A. The MSP shall ensure that the entire infrastructure is supported back-to-back by OEM's professional support services. The OEMs of the solutions proposed by the MSP shall provide the following support during the below mentioned phases:

1. Deployment Phase

a. Each OEM which are proposed by the MSP shall validate and certify the design, architecture, configurations, features enabled for their respective solutions proposed before installation and commissioning of the overall solution.

b. After completion of the deployment, OEMs shall again validate the design and certify the same as per best industry practices.

c. Each OEM shall assign single point of contact (SPOC) during the implementation phase.

2. Support Phase

a. The MSP should ensure that a robust support model is put together with OEM in such a way that the data centre runs with the level of availability as per the SLA as defined in Sr. No 5.

b. The MSP shall ensure the OEM's professional team develop a comprehensive support model for the contract period that will provide preventive, responsive and consultative support for all technological needs.

2.2.17 Training – Information Security and BCP

A. Operational training

1. The MSP shall impart operational training to all the designated resources, as and when needed. The modality and the group size of training will be mutually decided. This training should cover a session on security awareness, practices, and operations for the information security and BCP components installed at the Data Centre and Cloud
2. The standard contents of such training should be documented and made available to all the users. Changes to the same should be updated periodically as and when required and the same should be communicated to the respective sites.

B. Technical training

1. The MSP should also provide OEM technical training on all equipment to all the designated resources.
2. The training material should be designed specific to the participants.
3. The exact duration, schedule and coverage of such trainings shall be discussed with the MSP at the time of contract.

2.2.18 Documentation

A. The MSP shall be required to submit documentation in the format, media and number of copies as decided by Supreme Court of India. International standards and best practices to be followed while creating the documentation.

B. Indicative list of documents include:

1. The MSP shall submit the overall plan for deployment of complete solution as per the RFP, within 4 weeks of the award of contract which would be approved by

Supreme Court of India . The plan should include project plan in MS-Project giving out micro level activities with deadlines, HLD & LLD, layout design, approach methodology, onsite team deployment, test details and any other relevant details required for installation and configuration.

2. Documents related to the configuration, operation and maintenance of each and every security solution and services provisioned by the MSP. The document should cover all the procedures, policies and necessary information for diagnosis and repair of faulty units or components of every type.
3. The MSP shall make changes to the documents as and when there is change in the ICT infrastructure components or policies or as and when required by Supreme Court of India.
4. All the documents, manuals etc. would be solely owned by Supreme Court of India. Supreme Court of India reserves the right to verify the process and documentation submitted, at any given point of time.
5. The MSP shall be responsible for creation and maintenance of all the documentation including but not limited to configuration documents, network diagram, Data Centre operation manual, system administration manual, security administration manual, password management manual, etc. The servicing manual should cover all the procedures and information necessary for the diagnosis and repair of faulty units or components of every type.

2.2.19 Other Support Services

A. Maintain a record of all the hardware changes made in the ICT infrastructure solution.
B. Maintain the inventory of the entire hardware and software assets installed at the Data Centre.
C. The MSP shall maintain all documentation related to material movement of ICT and cloud infrastructure such as new hardware, spare parts or equipment going out of premises for repairing etc.
D. Schedule maintenance of the ICT infrastructure solution under the scope of work at the periodicity defined by the OEM and also as per the schedule defined in discussion with Supreme Court of India during the HLD and LLD discussions.
E. The MSP shall ensure implementation and enforcement of procedures, policies and guidelines like Security policy, Network access policy, Anti-virus policy, etc. as formulated in discussion with Supreme Court of India.
F. Supreme Court of India shall regularly monitor, audit and review the performance of complete services and manpower provided by MSP. Non-adherence to the required Service Level agreements shall attract penalty to the MSP.
G. The MSP shall ensure proper handover/ takeover of documents & other relevant materials in the event of change in personnel.
H. The MSP shall proactively interact with other vendors / third parties / OEMs to ensure that the equipment is upgraded and maintained at a periodic interval. The MSP would manage all aspects of Vendor management.
I. The MSP need shall extend support to the other MSP of Supreme Court of India and escalate incidents and issues to the respective MSP/suppliers of ICT infrastructure.

2.2.20 Final Acceptance Testing (FAT)

A. The final acceptance shall be considered completed after the successful testing by Supreme Court of India or its third-party monitoring agency; a Final Acceptance Test Certificate (FAT) shall be issued by Supreme Court of India. The date on which Final

FAT certificate is issued shall be deemed to be the date of successful commissioning of the overall solution and services provisioned by the MSP.

B. **Prerequisite for carrying out FAT activity:**

1. Detailed test plan shall be worked out by Supreme Court of India along with inputs from the selected MSP.
2. All documentation related to commissioned ICT infrastructure and relevant acceptance test documents should be completed & submitted before the final acceptance test to Supreme Court of India.
3. Deployment of Manpower as per the deployment proposed by the MSP in Annexure: Manpower/resource categories, skillset and qualifications.

C. **The FAT shall include the following:**

1. All the ICT hardware and software items must be configured at the site as per the project requirements.
2. Availability of all the defined services shall be verified.
3. The MSP shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
4. The MSP shall arrange the test equipment (if any) required for performance verification. The MSP will also provide test results.

D. The MSP shall be responsible for Acceptance schedules, detailed acceptance tests, formats for acceptance reports and dissemination mechanism for such reports shall be drawn by the MSP in consultation with Supreme Court of India.

E. The acceptance of the solution shall be provided by Supreme Court of India only after the following conditions have been met successfully to the satisfaction of NICSI.

1. Successful implementation, commissioning, and operation of the cloud solution
2. Completion of all the documentation required as part of this tender and as desired by Supreme Court of India.
3. Completion of the security audit of the overall solution and the services provisioned by the MSP. The security audit is to be carried out by a Cert-in empaneled certified auditor.

2.2.21 Constitution of the Team

A. All the proposed resources shall be deployed onsite at the date centre.

B. The MSP shall provide an adequate number of administrators, each responsible for its respective specific role at the Data Centre. The MSP must ensure the definition of the roles and responsibilities of each manpower resource as part of the Technical Bid as per the Annexure: Manpower/resource categories, skillset and qualifications.

C. Onsite resources will follow six working days per week cycle and will be entitled for all national holidays. If required resources would be called on holidays/odd hours, in such cases they will be entitled for compensatory leaves.

D. All the onsite resources deployed at DC must be on the MSP's payroll. Any third party payroll resource will not be accepted for onsite deployment.

E. All the concerned onsite staff shall log an attendance daily. The MSP shall maintain a database of attendance of the staff deployed at the Data Center. The attendance database should have facilities to track attendance and draw out MIS reports as desired by Supreme Court of India. The MSP shall submit the attendance records in a format and as per schedule desired by Supreme Court of India.

F. The police verification, character and antecedent's verification of the employees is the whole and sole responsibility of the MSP. The same may be verified by Supreme Court of India/ NICSI at the time of joining of the employees, if desired.

G. The MSP shall ensure the following in respect of his employees-

1. The working hours and days of the outsourced employees will be as per the existing applicable rules of Supreme Court of India. However, they have to work on extended hours and/or holidays, if necessary, based on the demand of work.
2. In the event of deployed personnel availing leave suitable substitute(s) shall be provided by MSP as per mutual understanding with Supreme Court of India.
3. On reporting poor performance of specific resources by Supreme Court of India MSP shall immediately replace such resources for maintaining service levels and continuity.

H. Timing for shifts and resource deployment:

- 06:00 AM to 02:00 PM : Minimum 2 resources
- 02:00 PM to 10:00 PM : Minimum 2 resources
- 10: 00 PM to 06: 00 AM : Minimum 2 resources
- 09:30 AM to 05:30 PM (General Shift): Minimum 1 specialized resource should be available for each skillset as defined in Annexure: Manpower/resource categories, skillset and qualifications.
- Minimum 2 resources should be available for each shift on Holidays and GH.
- Minimum 1 Redhat OpenStack onsite manpower (OEM certified)

2.2.22 Responsibilities of Supreme Court of India /NICSI

A. Supreme Court of India shall provide all the necessary basic (non IT) infrastructure such as cooling, power, DG and rack space etc.

B. Supreme Court of India shall provide approvals & signoffs to the deliverables within the stipulated time. Supreme Court of India shall direct and monitor the activities performed by the MSP as per the tender document and in turn validate the service levels attained as per the SLA defined at Sr. No 5.

3 Bidding Process

3.1 EMD

A. The Bidder shall furnish, as part of its bid, an Earnest Money Deposit (EMD) of an amount equal to 2% of the estimated value of the tender. All other Terms and conditions of GeM GTC shall be applicable.

3.2 Performance Bank Guarantee

A. The successful bidder shall furnish the performance bank guarantee (PBG) in the form of Bank guarantee within 15 days of the receipt of notification regarding the award of contract from the Purchaser. This PBG shall be as per the bellow schedule:

Sr.no.	Item	Value
1	Instrument	One single Deposit in the form of Bank Guarantee

2	Validity of Performance Bank Guarantee	Bank Guarantee should be valid for a period of 62 months. This PBG will be released on successful completion of all contract terms after deducting penalty (if any).
3	Amount	3% of the contract value

B. The Performance Bank Guaranty without any interest accrued, shall be released only after the expiry of the warranty period/ contract period of the solution successfully.

3.3 Bid Opening Process

A. Online bids (complete in all respect) received along with EMD will be opened in the presence of bidder's representative, if available. Bid received without EMD will be rejected straight way.

B. Technical bids of only those bidders, whose EMD is as per the format will only be evaluated further as per point "4. Evaluation Process" of the RFP.

4 Evaluation Process

A. NICSI will evaluate the responses of the bidder and all the supporting documents/ documentary evidence. Inability to submit requisite information may lead to rejection.

B. The decision of NICSI in the evaluation of proposals shall be final. No correspondence will be entertained outside the process of evaluation with NICSI. NICSI may call the bidder for meetings to seek clarifications or confirmations on their proposals.

C. NICSI reserves the right to reject any or all proposals. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.

4.1 Stage 1: Pre-qualification

A. Each of the Pre-Qualification condition mentioned in the Qualification Criteria is MANDATORY. In case the bidder does not meet any one of the conditions, the bidder will be disqualified and zero (0) marks will be awarded against each Technical Evaluation criteria as defined in Sr.No. 4.2.2. Technical Evaluation Criteria.

B. Bidder would be informed of their qualification/disqualification based on the pre-qualification.

C. If the bid is not accompanied by all the above-mentioned documents, the same may be rejected.

D. Undertaking for subsequent submission of any of the above document will not be entertained under any circumstances. However, NICSI reserves the right to seek required/additional documents (in case the bidder finds any issue, with due justification, in submitting the documents) and/or seek clarifications on the already submitted documents.

E. All documents should be submitted electronically in PDF format.

4.1.1 Prequalification Criteria

Sr. No.	Parameter	Clause	Documents Required
1	Legal Entity	The bidder should be an established Information Technology company registered under the Companies Act, 1956/2013 or LLP firm/ Partnership firm	• Valid documentary proof of: o Certificate of incorporation o Certificate of Commencement o Certificate consequent to change of name if applicable.

Sr. No.	Parameter	Clause	Documents Required
		under Partnership Act 1932 and in operation for at least 5 years as on 31.03.2023 and should have their registered offices in India. The company must be registered with appropriate authorities for all applicable statutory duties/taxes	○ Copy of Memorandum of Association • Valid documentary proof of: ○ GST Registration certificate ○ PAN Details ○ Income Tax returns for the last three financial years
2	Not Blacklisted	The bidder should not be actively blacklisted by any Central / State Govt. Ministry/ Department / PSU / Govt. Company. The Bidder should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice on the date of submission of the bid.	Self-certification duly signed by authorized signatory** on company letter head.
3	Annual Turnover	The bidder's average annual turnover should be at least (INR) 400 Cr. in the last seven Years. Note: Turnover from the group companies* can be considered	Certificate with CA's Registration Number and Seal.
4	Financial Turnover from ICT/ ICT enabled Services (ICTeS) / Data Centre/ Cloud	Turnover from ICT / ICTeS / DC / Cloud: Average turnover of the bidder from ICT / ICTeS / Data Centre Build or Operate / Cloud Services from last 3 financial years should be at-least INR 200 crores. **Note:** Turnover from the group companies* can be considered.	CA Certificate with CA's Registration Number and Seal
5	Relevant Experience in DC/Cloud	During the year last five years , the bidder must have must have an experience in setting up a modular data centre or cloud of at least 20 racks or two modular data centre or cloud of 10 racks	(a) Copy of work orders/contract agreement supported with relevant documentary evidence for the design parameters and the completion certificates by the client. Work order without completion certificate shall not considered.

<table>
<tr><th>Sr. No.</th><th>Parameter</th><th>Clause</th><th>Documents Required</th></tr>
<tr><td></td><td></td><td>each which includes activities such as
1. Supply, installation, configuration and commissioning of ICT infrastructure (Networking Equipment, Cyber Security, Storage and Backup Equipment, Servers)
2. Virtualizing ICT infrastructure
3. Providing support on the various application infrastructure in the datacentre / cloud.
4. Providing operations and maintenance services for the data centre/ cloud</td><td>or
(a) For bidder who have built their own Data Centre for commercial use will need to provide documentary evidence to justify commercial operation e.g., name of at least 5 client(s) who may be using the data centre services, list of services provided. Alternatively, in the case of NDA, bidder shall submit a declaration signed by the Authorized Signatory** of the bidder mentioning details of such clients along with supporting documents. However, in case if any content in the supporting document is masked, NICSI reserves the right to call for original document for its verification and the bidder shall comply with the same.
(b) Certificate with CA’s Registration Number and Seal on confirming the invested value.</td></tr>
<tr><td>7</td><td>Net Worth</td><td>The Net Worth of the bidder as of the end of the latest financial year (i.e., FY 2022-23) should be positive.
Note: The net worth of the parent company OR collective net-worth of group companies* shall be considered.</td><td>Certificate with CA’s Registration Number and Seal.</td></tr>
<tr><td>8</td><td>Resources/ Manpower Strength of Bidder</td><td>As on 31st March 2023, the bidder should have on its roll at least 50 employees working in datacentre/ cloud/ ICT/ managed services business.</td><td>Certificate from bidder’s HR Department for the number of Technically Qualified professionals employed by the company. Certificate should capture employee’s following details:
<table><tr><td>Employee name</td><td></td></tr><tr><td>Partially Masked PF no.</td><td></td></tr><tr><td>Qualification:</td><td></td></tr><tr><td>Years of Experience</td><td></td></tr><tr><td>Designation / Domain of expertise</td><td></td></tr></table></td></tr>
</table>

Sr. No.	Parameter	Clause	Documents Required
9	OEM MAF	The bidder should submit valid letter from all the OEMs confirming the following: o Authorization for bidder to confirm that the products quoted are not "end of life or end of sale products". o Undertake that the support including spares, patches for the quoted products shall be available for next 7 years.	Documentary evidence's such as Manufacturers Authorization Form (MAF) from all OEMs whose products are being quoted.
10	OEM Capability	(a) Hardware OEM : must have direct or registered service partner presence in India with **at least ten (10) nos. of technical manpower** in India for the offered technology solution(s). (b) Software OEM: must have direct or registered service partner presence in India with **at least five (5) nos. of technical manpower** in India for the offered technology solution(s).	(a) An undertaking from each OEM for the requisite number of technical manpower for direct support in India (b) Work order/Contact agreement etc.
11	Certification	The bidder must have at least three of the following certifications for their datacentre with the first two certificates being mandatory: a) ISO 27001:2015/2013 b) ISO 20000-1:2018 c) ISO 9001:2015 d) ISO 27017:2015 e) ISO 27018:2019 f) ISO 22301:2019 g) PCI-DSS h) SOC 2 Type 2 audit i) CMMi L3 or above	Valid Copy of the Certification stating the location and the scope of the certification

Sr. No.	Parameter	Clause	Documents Required
12	Office in consignee location	The bidder should have a project/local office in the 'Consignee Locations', i.e., Delhi	An undertaking in this regard must be provided by the bidder on its company letter head (having address and contact person details of project/local office) duly signed and stamped by the authorised signatory**. In case, bidder does not have existing project/local office in all the consignee locations, bidder must produce an affidavit by the authorized signatory committing to start a local office within 30 days of award of contract.
13	Point of Contact	The bidder shall be the single point of contact and shall be solely responsible for all warranties and upgrades etc.	Self-certification duly signed by authorized signatory** on company letter head.
14	IT Act	The bidder must comply with IT Act 2000 (including 43A) and all latest amendments.	Self-certification duly signed by authorized signatory** on company letter head. Self declaration from the Authorized signatory of the bidder on their letterhead.

Note:

A. *Group Company: A group as defined in Accounting Standard (AS) 21 or the companies whose majority shareholding is with the same common promoters#. In this case, the bidder needs to submit:
   1. CA certificate showing the common shareholding of the promoters in the bidder entity (agency) and all such entities whose credentials are being used by the bidder(agency).
   2. Certificate from a CA on the total turnover and net worth of such entities after having examined audited books of accounts of the entities (with common promoter) whose credentials are being used by the bidder (agency).
   3. An undertaking by the promoter# of such common entities as per the format.
   4. #Promoter(s) refers individual and his/her relatives as defined under the provisions of the companies act 2013 and the rules notified there under.

B. **Authorised Signatory: Chairman, CEO, CTO or MD level authority or CA having name, address, contact number and e-mail address or Authorised signatory with a Power of Attorney.

C. For the Financial Qualification requirements of sales turnover, data provided by the Bidder in foreign currency, equivalent Indian Rupees will be calculated using exchange rates USD/INR as available on website of Reserve Bank of India prevailing on the date of closing of the accounts for the respective financial year as certified by their banker.

D. If the exchange rate for any of the above dates is not available, the rate for the immediately available previous day shall be considered.

E. For the projects executed in the current financial year exchange rate USD/INR of Reserve Bank of India prevailing on seven (7) days prior to the last date of submission of bid to RFP and as certified by their banker shall be considered.

4.2 Stage 2: Technical Evaluation

4.2.1 Technical Evaluation Framework

A. Details of equipment and Technical Specifications/requirement to be procured are given in "**Annexure: Technical Specification"**.

B. List of Enclosures submitted should be properly numbered and indexed along with signatures of the authorized representative of the bidder. The bidder should ensure the following while submitting their bid:

1. Necessary detailed technical write up should highlight key points of the solution provided.
2. Any other document which the vendor may consider necessary to support the product /bid may be submitted.
3. All documents should be submitted electronically in PDF format.

C. Only those bidders who qualify all Pre-qualification Criteria requirements will be qualified for technical bid evaluation.

D. NICSI reserves the right to reject a Product/Solution/Service if it is of an opinion that the offered product/service does not match the technical requirements/objectives of the RFP.

E. Any bid found to be non-compliant to the mandatory technical requirements, tender terms & conditions and the scope of work shall be rejected and will not be considered for further evaluation. Bids that are technically compliant would only be taken up for commercial evaluation. Representations, if any from disqualified bidder will not be entertained and will be summarily rejected. NICSI will not entertain to any query raised by bidder seeking reasons for rejection of the bid.

F. NICSI reserves right to summarily reject any bid which does not contain all the mandatory supporting document or may ask bidder to resubmit documents, the decision of NICSI will be final and binding in this regard.

G. The Technical Evaluation process is as mentioned below:

1. Bidder should submit detailed documents and relevant evidence for: Bidder's Experience; Proposed Solution Approach & Methodology, Resource planning; Project Governance, Project Management, Success Story, response to **Annexure: Technical Specification** and solution document would be critical and decision of NICSI on these documents are binding the Bidder.
2. NICSI reserves the right to request the bidder to conduct a Proof of Concept (PoC)) /Prototype and live technical demonstration of the desired component(s) of the product(s) and/or solution(s) or a reference site visit for the proposed technology/solution. Time, Material and Cost so involved for this exercise would be borne by the bidder without any liability to the consignee.
3. No request for time extension shall be entertained regarding the deployment of Prototype /Demonstration. Hence, the bidder may start working and mobilise required key resources for the arrangement of Prototype Deployment/Demonstration from the date of publishing of the RFP in the background.

4. The Bidders would be assigned marks for each of the criteria as mentioned in Sr. No 4.2.2 of the Technical Evaluation Criteria. Bidder has to score 70% in each section and overall, 70% would be the qualifying marks to qualify for next level.
5. All the Bidder qualifying or not qualifying for Technical Evaluation will be notified via e-procurement portal/e-mail.

4.2.2 Technical Evaluation Criteria

Technical bids will be evaluated for the following broad parameters:

Sr. No.	Technical Evaluation Criteria	Criteria	Cut off Marks	Max. Marks	Supporting documents to be submitted
1	Financial Capability of the Agency	Average annual turnover of the agency in last Seven years i. Turnover of Rs. 400 Cr = 7 Marks ii. Apart from clause (i), if the bidder submits any additional turnover value of Rs. 50 Cr, additional 1 mark will be awarded for each 50 Cr	7	10	Turnover certificate from CA with CA's Registration Number and Seal
2	Financial Turnover from ICT/ ICT enabled Services (ICTeS) / Data Centre/ Cloud	Turnover from ICT / ICTeS / DC / Cloud: Average turnover of the bidder from ICT / ICTeS / Data Centre Build or Operate / Cloud Services from last 3 financial years should be at-least INR 200 crores. i. Turnover of INR 200 Cr. = 14 Marks ii. Apart from clause (i), if the bidder submits any additional turnover value exceeding Rs. 20 Cr, additional 1 mark will be awarded for each INR 20 Cr	14	20	Turnover certificate from CA with CA's Registration Number and Seal
3	Relevant Experience in DC/Cloud	During the year last five years , the bidder must have an experience in setting up modular data centres or cloud of	14	20	Copy of work orders/contract agreement

Sr. No.	Technical Evaluation Criteria	Criteria	Cut off Marks	Max. Marks	Supporting documents to be submitted
		i. Total 20 racks = 14 marks ii. Apart from clause (i), if the bidder submits any work order of datacentre/ cloud having racks more than 20 racks then for each additional 5 racks within the same workorders, additional 1 mark shall be awarded.			
4	Technical Resources/ Manpower Strength	Technically qualified professionals exclusively working in data centre/ cloud and managed services business i.e., cloud automation, cyber security, networking, system software, systems integration, storage, cloud solutions. Present strength of manpower on the bidder's payroll, as on bidding date: i. 50 - 75 resources – 7 marks ii. 76 to 100 resources – 8 marks iii. 101 or 150 resources – 9 marks iv. 151 and above – 10 marks Note 1: Bidder will be considered only in one of the above-mentioned categories Note 2: Manpower of subsidiaries companies will not be considered	7	10	An undertaking in this regard must be provided by the agency on its company letter head duly signed and stamped by the authorized signatory**

Sr. No.	Technical Evaluation Criteria	Criteria	Cut off Marks	Max. Marks	Supporting documents to be submitted
5	Certifications	The bidder's data centre or any client data centre which has been built or is being operated by the bidder shall be evaluated on the basis of the number of certifications it possesses. The list of certifications are as follows: a) ISO 9001:2015 b) ISO 27001:2013 c) ISO 27001:2015 d) ISO 27017:2015 e) ISO 27018:2019 f) ISO 20000-1:2018 g) ISO 22301:2019 h) PCI-DSS i) SOC 2 Type 2 audit j) CMMI L3 or above i. 3 Certificates – 7 marks ii. for each certificate 1 marks each	7	10	Valid Copy of the Certification stating the location and the scope of the certification
6	Technical presentation	Technical presentation shall be evaluated based on the points mentioned in D of the Note below.	21	30	

Note:

A. Value of work order will be considered as inclusive of all taxes.
B. Subsequent work orders (W/O), in continuation of existing work orders, for any project will be considered as a single W/O
C. Turnover and experience from the group companies can be considered. The agency shall provide necessary supporting documents to provide relation with parent company/ group company.
D. The technical presentation shall be evaluated based on the following broad parameters. (Each parameter carries 3 marks)
    1. Past experience related to the current scope of work, data centre security and mitigation plans.
    2. Proposed product/solution capability.
    3. Understanding of the proposed Scope of work and the Proposed approach & methodology of the bidder

4. Availability of the support infrastructure and technology lab of the proposed OEMs within the country.
5. Qualification and expertise of the proposed onsite technical team along with team size .
6. Plan for SLA adherence and spare parts provisioning
7. Action plan on the various severity levels along with escalation matrix for each severity, incidents and SLA
8. Centralized dashboard and reporting
9. Bidder's forecast on challenges along with mitigation plan
10. Exit Management Plan

4.3 Total Bid Evaluation

A. The evaluation of the tender is based on **QCBS (Quality and Cost Based Selection)**.

B. Technical score shall have a weightage of 70 % and commercial score shall have a weightage of 30%.

C. The Final score (FS) of the bidder = 0.7*(Technical Score) + 0.3*(Financial Score)

5 Award of the Contract

5.1 Delivery, Installation and Commissioning Timelines

SL. No	Activity	Timeline in Weeks
1	Delivery of Equipment	Within 8 weeks from the date of acceptance of the Contract
2	Installation ,Commissioning and integration of the ICT infrastructure.	Within 4 weeks from the date of delivery
Note: 1. Date of award of contract shall be herein after referred as T.		

5.2 Payment Terms

A. A pre-received bill (Three copies) shall be submitted in the name of "NATIONAL INFORMATICS CENTRE SERVICES INC" at NICSI, New Delhi.

B. MSP has to install all the ordered items and will prepare the installation report as per the prescribed format and get it signed by the concerned In-charge or his/her authorized person/NICSI officer with date and stamp. For the overall project commissioning, a duly signed FAT certificate shall be submitted.

C. MSP must provide all necessary documentation related to services consumed, O&M and data migration efforts and any other documents as demanded by Supreme Court of India/ NICSI and as mentioned in this RFP. Invoice without any of the above-mentioned documents shall be called as incomplete and shall not be accepted.

D. If the MSP fails to install the ordered equipment within a given time, penalty as per Penalty Terms as defined in Sr. No 5.3 shall be applicable.

E. All payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the latest Income-Tax Act and GFR 2017.

5.2.1 Payment for Hardware Items

A. Payment will be made for hardware items as defined in Annexure: Un-priced BOQ, as per the following schedule:

1. **70% of the lot value on the delivery** for all the items under a lot as defined in **Annexure: Un-priced BOQ.**
2. **30 % of the total value of the hardware and software deliverables on the completion on the completion of all deliverables of the contract**; as well as upon the submission of duly signed FAT.

5.2.2 Payment for Software Items

A. Payment for Software Items i.e., subscription and support charges as defined in **Annexure: Un- Priced BOQ** will be made annually at the starting of each year.

5.2.3 Payment terms for Yearly Support/ AMC charge

Yearly Support/ AMC Charges will be made quarterly at the end of each quarter.

5.2.4 Payment for Operation & Maintenance

Payment for Operation and Maintenance will be made on quarterly basis at the end of the quarter based on the quarterly performance report and manpower attendance report duly signed by the concerned In-charge or his/her authorized person. The Operation and Maintenance shall start after the submission of the duly signed FAT.

5.3 Penalty Terms

5.3.1 Penalty for Late Delivery of ICT Infrastructure

A. Delivery of all the quoted ICT infrastructure components shall be completed within stipulated timeline. Lot-wise list of components is available in the Annexure: Un-priced BOQ.

B. Penalty shall be charged for each item not delivered on time, as per the below table.

Required Delivery Time	Delivery Time	Penalty
T + 8 Weeks	T + 9 Weeks	2% of PO value
	T + 10 Weeks	4% of PO value
	T + 11 Weeks	6% of PO value
	T + 12 Weeks	8% of PO value
	T + 13 Weeks	10% of the PO value
	T + 14 Week	NICSI may opt for order cancellation and revocation of Bank Guarantee (PBG)
Note: 1. MSP shall provide a valid business reason to Supreme Court of India /NICSI for delay in delivery. If no valid reason and/or effect of force majeure condition is established, then Supreme Court of India/NICSI may choose to revoke the MSP's PBG.		

5.3.2 Penalty for Installation, commissioning of the of ICT Infrastructure

A. Installation of all ICT infrastructure listed in **Annexure: Un-priced BOQ** shall be completed within stipulated timeline.

Required commissioning time	Actual commissioning time	Penalty
T_1 + 4 Weeks	T_1 + 5 Weeks	2% of contract value

	T_1+ 6 Weeks	4% of contract value
	T_1+ 7 Weeks	6% of contract value
	T_1+ 8 Weeks	8% of contract value
	T_1+ 9 Weeks or beyond	10% of the contract value

Note:

1. T_1 is the date of delivery of the respective equipment/solution.
2. Exemption in delay due to site-not-ready will be considered on submission of Annexure: Site not ready certificate issued by the concerned site in-charge is submitted.
3. MSP shall provide a valid business reason to Supreme Court of India/NICSI for delay in Installation. If no valid reason and/or effect of force majeure condition is established, then Supreme Court of India / NICSI may choose to revoke the MSP's PBG.

5.3.1 Penalty for unauthorized absence of onsite resources

A. If any onsite resource deployed is absent without the consent of Supreme Court of India, a penalty at the rate of Rs. 1000 per day of absence shall be levied on the MSP. The penalty shall be deducted from the quarterly payments due.

5.3.2 Penalty for Non-Adherence to Service Level Agreement for Cloud Infrastructure Operations

A. Please refer to Sr. No 6 SLA for detailed deliverables, uptime requirement of services and respective penalties.

5.3.3 Overall Penalty for Supply, Installation and Commissioning of ICT Infrastructure

A. The section wise penalty on the Delivery of the ICT infrastructure is capped at 10% whereas the overall penalty on account of delay in supply, installation , configuration and commissioning of the overall solutions shall not exceed 20% of the contract value.

5.4 Exit Management

A. The MSP would be part of the operation team of a critical/essential of Government of India and the project is strategic in nature and impacting Government functions. It is necessary to have a comprehensive exit management strategy in place. Supreme Court of India /NICSI will take all steps required for selecting a new MSP before the end of current contract . However, the incumbent MSP should ensure continuation of services till an alternative is in place and will ensure smooth transition. However, in exceptional circumstance, the contract can be extended on mutual consent , up to a maximum period of two years or till the appointment of a new MSP whichever is earlier, on existing terms and conditions.

B. The MSP shall need to ensure the following:

1. The MSP shall submit a structured & detailed exit management plan along with the technical proposal.
2. Exit Management Plan shall be presented by the MSP and approved by Supreme Court of India /NICSI or its nominated agencies.

3. The MSP needs to update the exit management on a half yearly basis or earlier in case of major changes during the entire contract duration. This plan needs to be discussed and approved by the Supreme Court of India/NICSI.
4. The MSP shall also submit a technical plan for transfer of applications, data, backup media, documentation, and any other asset of Supreme Court of India/ NICSI in case Supreme Court of India /NICSI decides not to continue further with the MSP. The MSP shall facilitate all such transfer with the chosen service provider of Supreme Court of India /NICSI.
5. At the end of the contract period or during the contract period, if any other agency is identified or selected for providing services related to the MSP's scope of work, the MSP shall ensure that a proper and satisfactory handover is made to the other agency. MSP will support in all respects and decision of Supreme Court of India / NICSI shall be final in this regard.
6. All risks during the transition stage shall be properly documented by the MSP and mitigation measures shall be planned to ensure a smooth transition without any service disruption.
7. Closing off all outstanding/open issues as on date of exit and the same to be listed and provided to Supreme Court of India /NICSI.
8. The MSP shall provide necessary knowledge transfer and transition support. The deliverables are indicated below:
    a. Complete documentation for the entire system handed over to Supreme Court of India /NICSI identified agency.
    b. Handover of all AMC support related documents, credentials etc. for all OEM products supplied/maintained in the system. Handover MOUs signed for taking services taken from third parties such as digital signature agencies, etc.
    c. Handover of the list of complete inventories of all assets inclusive of digital assets created for the project.
    d. Assisting the new agency/ Supreme Court of India /NICSI with the complete audit of the system including licenses and physical assets.
    e. Detailed walk-throughs and demos for the solution. Hand-over of the user IDs, passwords, security policies, scripts etc.
9. Knowledge transfer of the system to the incoming MSP to the satisfaction of the new MSP as per the timelines which will be specified by Supreme Court of India /NICSI.
10. The MSP shall be released from the project once successful transition is completed by meeting the parameters defined for successful transition.
11. The commercial quoted by the MSP shall include transition costs also and Supreme Court of India / NICSI will not pay any additional fees for transition.
12. During Exit, the MSP shall indemnify losses completely, if any, to the Supreme Court of India /NICSI and shall meet all the obligations towards Supreme Court of India /NICSI, Third Party Service providers, OEMs etc. before handing over the infrastructure and clients to Supreme Court of India/ NICSI.
13. The assets shall be free from any financial obligations owing to any of the financial institutions/banks, clients, service providers etc.

5.4.1 Transfer of Project Assets

A. Before the expiry of the Exit Management Period, all Project Assets including the hardware, software, system software documentation and any other infrastructure shall have been renewed and cured of all defects and deficiencies as necessary so that the Project is compliant with the specifications and standards set forth in the Agreement, RFP, and any other amendments made during the Contract Period.

B. Before the expiry of the exit management period, the MSP will deliver relevant records and reports pertaining to the Project and its design, implementation, operation, and maintenance including all operation and maintenance records and manuals pertaining thereto and complete as on the divestment date to Supreme Court of India /NICSI.

C. The MSP will provide the Supreme Court of India / NICSI with a complete and up to date list of the Assets to be transferred to the Supreme Court of India's appointed agency within 30 days of start of Exit Management Period.

D. The outgoing MSP will pass on to Supreme Court of India / NICSI and/or to the replacement agency (if engaged by the Supreme Court of India / NICSI), the subsisting rights in any leased properties/ licensed products on terms not less favourable to the Department/ replacement agency, than that enjoyed by the outgoing Bidder.

5.4.2 Employees

A. Promptly on request at any time during the exit management period, the MSP shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to Supreme Court of India / NICSI a list of all employees (with job titles and communication address) of the MSP, 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 MSP, Supreme Court of India / NICSI or Replacing MSP may make an offer of contract for services to such employee of the MSP and the MSP shall not enforce or impose any contractual provision that would prevent any such employee from being hired by Supreme Court of India / NICSI or any Replacing MSP.

6 Service Level Agreement & Penalty

A. Once the contract is awarded, the MSP shall not refuse to accept the same. In case of refusal by the MSP, NICSI/ Supreme Court of India may revoke the Performance Bank Guarantee or EMD.

B. The MSP shall centrally monitor and manage the devices on a 24x7x365 basis to ensure an uptime of 99.98% for all the ICT infrastructure and 99.95% for all the cloud services for the cloud setup as per the defined SLAs of this RFP.

C. The MSP shall ensure services at a level of excellence which matches with the Scope of Work requirements as defined in Sr. No 1 of the RFP.

D. The MSP shall render the services strictly adhering to the SLAs mentioned in this section and Delivery, Installation and Commissioning timelines as defined in Sr.No 4.1. Any delay, not condoned by Supreme Court of India / NICSI, on the part of MSP in the performance of its obligations shall attract penalty. Post that Supreme Court of India / NICSI will have the option of getting the work done through alternate sources at the cost and risk of the MSP, which will be realized from pending payments of the MSP, or from the Performance Bank Guarantee or by raising claims.

E. The MSP shall maintain spare units at appropriate locations to meet the service level agreement (SLA) requirements.

F. Any unjustified and unacceptable delay resulting from reasons attributable to the MSP beyond the schedule will render the agency liable for penalty as defined in this section.
G. Defective equipment supplied / leased by the MSP shall be repaired / replaced by the MSP without any additional cost.
H. Any system, failing at subsystem level at least three times in three months, displaying chronic system design or manufacturing defects or quality control problems will be totally replaced by the MSP with same or higher specification, of the same OEM or a different OEM (if Supreme Court of India /NICSI deems necessary) at their own cost and risk within 30 days, from the date of last failure. If the MSP fails to replace the system within 30 days, penalty will be charged at the rate of 0.2% (Zero-point two percent) of system purchase value per day per system up to a maximum value of 10% (Ten percent) of the purchase order.
I. Root cause analysis of any service ticket has to be done and proper corrective action has to be taken with information to Supreme Court of India / NICSI / User Location officials.
J. If the service call is not resolved within the stipulated time period, this would be treated as deficiency in service and terms & conditions pertaining to deficiency in service would be applicable.
K. The penalty may be recovered from the quarterly payment or Performance Bank Guarantee or by raising claims.
L. Any recovery of penalty shall not in any way relieve the MSP from any of its obligations to complete the works/services or from any other obligations and liabilities under the SLA.
M. Supreme Court of India / NICSI reserve the right to levy / waive off penalty considering various circumstances at that point in time.
N. If at any time during performance of the work order, the MSP encounter conditions impeding timely performance of the ordered services, the MSP shall promptly notify Supreme Court of India /NICSI in writing of the fact of the delay, it's likely duration and its cause(s)
O. For non-execution of work orders for reasons attributable to the MSP, Supreme Court of India / NICSI would be free to use defaulting agency's Performance Bank Guarantees received against the affected work order and/or termination of the Contract provided agency fails to remedy such default in spite of 30 days written notice from Supreme Court of India/NICSI to cure such default.
P. The general terms w.r.t the service level agreement is defined as mentioned below.
    1. The uptime for the infrastructure would be calculated on monthly basis.
    2. The uptime calculation will be done as per the formula given below:
        a. Uptime (%) = (Sum of total hours during month – Sum of downtime hours during month) X 100 / Sum of total hours during month
        b. Total hours in a month will be taken as: 24 hrs X no. of days in respective month.
Q. Penalty Calculation Matrix for ICT Equipment:

1. Penalty for Service and Equipment Failure (for the Data Center ICT infrastructure components supplied and installed under this project) shall be calculated on the basis of total service failure and individual equipment/part. In case when both total service failure and individual equipment/part failure are applicable the higher one shall be charged. Penalty for service and equipment failure shall be deducted from the quarterly dues to the MSP.
2. The Penalty shall be calculated on a quarterly basis. The Penalty would be calculated on an incremental basis for each component of the entire ICT Infrastructure affected. For example, if the total number of Leaf Switch affected is 3, the Penalty would be

multiplied by 3. If downtime of system or subsystem affects the operation of other systems, then vendor has to pay penalty for the affected systems also.

3. The downtime shall be the time from the point the respective equipment becomes unavailable (due to any reason attributable to the Bidder) till the time the same becomes fully available for carrying out intended operations (including reinstallation, configuration, restoration, boot-up time, etc.) OR till the time a standby equipment is made available for carrying out intended operations (including installation, configuration, restoration, boot-up time, etc.)

Sr. No	Failure	Target (Quarterly)	Impact	Penalty
1.	Total Service failure of the ICT equipment	99.98%	26 minutes and 5 seconds downtime	No Penalty
		>= 99.95% to < 99.98%	<= 1 hour 5 minutes > 26 minutes and 5 seconds of downtime	1 % of the Purchase order value of failed ICT equipment/service.
		>= 99.95% to < 99.9%	<= 2 hours 10 minutes> 1 hour 5 minutes of downtime	3 % of the Purchase order value of failed ICT equipment/service.
		< 99.9%	> 2 hours 10 minutes of downtime	5 % of the Purchase order value of failed ICT equipment/service
2.	ICT equipment failure (Loss of redundancy but not leading to service failure)	99. 8%	4 hour 20 min	No Penalty
		>= 99.8% to < 99.5%	<=4 hour 20 min >10 hour 52 min	0. 5% of the Purchase order value of failed ICT equipment.
		>= 99. 5% to < 99.0%	<= 10 hour 52 min > 21hour 44min	0. 8% of the Purchase order value of failed ICT equipment.
		< 99.0%	> 21hour 44min	0. 7% of the Purchase order value of failed ICT equipment
3.	Equipment's component Failure (not leading to failure defined at Sr. No. 1 & 2 in this Table)	99.0%	21hour 44min	No Penalty
		>= 99.0% to < 98.5%	<= 21hour 44min > 1 day 8 hours of downtime	0.1% of the Purchase order value of failed ICT equipment.
		>= 98.5% to < 98.0%	<= 1 day 8 hours > 1 day 19 hours of downtime	0.3% of the Purchase order value of failed ICT equipment.
		< 98.0%	> 1 day 19 hours of downtime	0.5% of the Purchase order value of failed ICT equipment

R. The MSP shall adhere to the following SLA matrix for operation and management of the cloud:

Sr. No	Service Level Objective	Definition	Target	Penalty
1	Availability of cloud service	Availability means, the aggregate number of hours in a calendar month during which cloud service is actually available for use through command line interface, user/admin portal and APIs (which ever applicable) Uptime Calculation for the calendar month: (Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability of the cloud service>=99.95%	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.9 % - 5% of Quarterly Payment due to the MSP b) <99.9% to >= 99.5%- 10% of Quarterly Payment due to the MSP c)<99.5% to >= 99% - 15% of Quarterly Payment due to the MSP d) <99% - 20% of the Quarterly Payment due to the MSP
2	Provisioning of new Virtual Machine	Time to provision new Virtual Machine (up to 64 core) Measurement shall be done by analysing the log files	95% within 30 Minutes	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 1% of Quarterly Payment due to the MSP b) <90% to >= 85.0% - 5% of Quarterly Payment due to the MSP c) <85% to >= 80.0% - 8% of Quarterly Payment due to the MSP d) <80% - 10% of the Quarterly Payment due to the MSP
3	Spinning up the Object Storage	Time to spin up Object Storage. Measurement shall be done by analysing the log files	98% within 30 minutes	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 1% of Quarterly Payment due to the MSP

Sr. No	Service Level Objective	Definition	Target	Penalty
				b) <95% to >= 90.0% - 5% of Quarterly Payment due to the MSP c) <90% to >= 85.0% - 8% of Quarterly Payment due to the MSP d) <85% - 10% of the Quarterly Payment due to the MSP
4	Spinning up the Unified Storage	Time to spin up to 100 GB Block Storage and attach it to the running VM. Measurement shall be done by analysing the log files	98% within 30 minutes	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 1% of Quarterly Payment due to the MSP b) <95% to >= 90.0% - 5% of Quarterly Payment due to the MSP c) <90% to >= 85.0% - 8% of Quarterly Payment due to the MSP d) <85% - 10% of the Quarterly Payment o due to the MSP
5	Usage metric for all Cloud Services	The usage details for all the Cloud Service should be available within 15 mins of actual usage Measurement shall be done by analysing the log files and Cloud Service (API) reports.	No more than 15 minutes lag between usage and Cloud Service (API) reporting, for 99% of Cloud Services consumed by the Government Dept.	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of Quarterly Payment due to the MSP b) <95% to >= 90.0% - 2% of Quarterly Payment due to the MSP c) <90% to >= 85.0% - 3% of Quarterly Payment due to the MSP d) <85% - 5% of

Sr. No	Service Level Objective	Definition	Target	Penalty
				the Quarterly Payment due to the MSP
6	Usage cost for all Cloud Service	The cost details associated with the actual usage of all the Cloud Service should be available within 24Hrs of actual usage Measurement shall be done by analysing the log files and Cloud Service (API) reports and Invoices	No more than 24 Hrs. of lag between availability of cost details and actual usage, for 99% of Cloud Services consumed by the Government Dept.	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of Quarterly Payment due to the MSP b) <95% to >= 90.0% - 2% of Quarterly Payment due to the MSP c) <90% to >= 85.0% - 3% of Quarterly Payment due to the MSP d) <85% - 5% of the Quarterly Payment due to the MSP
7	Percentage of timely vulnerability reports	Percentage of timely vulnerability reports shared by CSP/MSP within 5 working days of vulnerability identification. Measurement period is calendar month.	Percentage of timely vulnerability reports-shared within 5 working days of vulnerability identification>= 99.95%	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 1% of Quarterly Payment due to the MSP b) <99.00% to >= 98.00% - 3% of Quarterly Payment due to the MSP c) <98% - 5% of Quarterly Payment due to the MSP
8	Percentage of timely vulnerability corrections	Percentage of timely vulnerability corrections performed by CSP/MSP. a) High Severity - Perform vulnerability correction within 30 days of vulnerability identification. b) Medium Severity - Perform vulnerability correction within 60 days	Maintain 99.95% service level	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 1% of Quarterly Payment due to the MSP b) <99.00% to >= 98.00% - 3% of Quarterly Payment due to the MSP

Sr. No	Service Level Objective	Definition	Target	Penalty
		of vulnerability identification. c) Low Severity - Perform vulnerability correction within 90 days of vulnerability identification. Measurement period is calendar month		c) <98% - 5% of Quarterly Payment due to the MSP
9	Security Incident (Malware Attack / Denial of Service Attack / Intrusion or Defacement)	Security incidents could consist of any of the following: Malware Attack: This shall include Malicious code infection of any of the resources, including physical and virtual infrastructure and applications. Denial of Service Attack: This shall include non-availability of any of the Cloud Service due to attacks that consume related resources. The MSP shall be responsible for monitoring, detecting and resolving all Denial of Service (DoS) attacks. Intrusion: Successful unauthorized access to system, resulting in loss of confidentiality / Integrity / availability of data. The MSP shall be responsible for monitoring, detecting and resolving all security related intrusions on the network using an Intrusion Prevention device.	a) Any Denial-of-service attack shall not lead to complete service non-availability. b) Zero Malware attack / Denial of Service attack / Intrusion	For each occurrence of any of the attacks (Malware attack / Denial of Service attack / Intrusion / Data Theft), 10% of the Quarterly Payment of the Project
11	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 95% of the incidents should be resolved within 15	) <95% to >= 90.00% - 1% of Quarterly Payment due to the MSP

Sr. No	Service Level Objective	Definition	Target	Penalty
			minutes of problem reporting	b) <90% to >= 85.00% - 2% of Quarterly Payment due to the MSP c) <85% to >= 80.00% - 3% of Quarterly Payment due to the MSP d) Subsequently, for every 5% drop in SLA criteria – additional 2% of Quarterly Payment due to the MSP
12	Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 60 minutes of problem reporting AND 95% of Severity 3 within 2 hours of problem reporting	a) <95% to >= 90.00% - 0.5% of Quarterly Payment due to the MSP b) <90% to >= 85.00% - 1% of Quarterly Payment due to the MSP c) <85% to >= 80.00% - 1.5% of Quarterly Payment due to the MSP d) Subsequently, for every 5% drop in SLA criteria – additional 1% of Quarterly Payment due to the MSP
13	Line Item has been removed			

Sr. No	Service Level Objective	Definition	Target	Penalty
14	Data Migration	Migration of data from the source to destination system	Error rate < .25%	a) Error Rate > 0.25% &<=0.30% - 1% of the Quarterly Payment due to the MSP b) Error Rate > 0.30% &<=0.35% - 2% of the Quarterly Payment due to the MSP c) Error Rate > 0.35% &<=0.40% - 3% of the Quarterly Payment due to the MSP For each additional drop of 0.05% in Error rate after 0.40%, 1% of Total Quarterly Payment of the Project will be levied as additional liquidity damage
15	Patch Application	Patch application and updates to underlying infrastructure and cloud service Measurement shall be done by analysing security audit reports	95% within 8 Hrs. of the notification	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 1% of Quarterly Payment due to the MSP b) <90% to >= 85.0% - 2% of Quarterly Payment due to the MSP c) <85% to >= 80.0% - 4% of Quarterly Payment due to the MSP d) <80% - 5% of the Quarterly Payment due to the MSP
16	Budget Alerts & Notification	Alerts and Notifications for budgeting and usage-based threshold Measurement shall be	99% within 10 mins of crossing the Threshold	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 0.25% of

Sr. No	Service Level Objective	Definition	Target	Penalty
		done by analysing the log files		Quarterly Payment due to the MSP b) <95% to >= 90.0% - 0.5% of Quarterly Payment due to the MSP c) <90% to >= 85.0% - 0.75% of Quarterly Payment due to the MSP d) <85% - 1% of the Quarterly Payment due to the MSP
18	Time taken for generation of Root Cause Analysis (RCA) report for incidents of Severity 1, 2, and 3	The scope includes all the incidents of Severity 1, 2 & 3 in the reporting period. Definition: Time taken for generation of Root Cause Analysis (RCA) report for incidents of Severity 1, 2 and 3 Calculation: Measurement shall be done for all RCA reports submitted within the quarter and within the prescribed time limits. Each RCA report shall be treated individually. SLA Calculation Formula: All the [Severity 1, 2 and 3] RCA to be submitted within 48 hours after restoration of affected services. Target: Time taken for generation of Root Cause Analysis (RCA) report for incidents of Severity 1, 2, and 3 <=48 hours	<=2 days (48 hrs)	NIL
			> 2 days (48 hours)	Penalty as indicated below (per occurrence): a) <2 days to >= 4 days - 0.25% of Quarterly Payment due to the MSP b) <4 days to >= 6 days - 0.5% of Quarterly Payment due to the MSP c) <6 days to >= 8 days - 0.75% of Quarterly Payment due to the MSP d) <8 days - 1% of the Quarterly Payment due to the MSP

Sr. No	Service Level Objective	Definition	Target	Penalty
		If any RCA is not submitted within the target time mentioned above for any given month, then this SLA will be considered as breached. RCA is applicable only for Severity 1 and 2 incidents, rest can be considered as part of problem management policies or procedures.		

S. The section wise penalty for operation and management of cloud is capped at 10% whereas the overall penalty on the MSP shall not exceed 20% of the quarterly payment.

T. The MSP shall be responsible for any security breach of the ecosystem deployed by the MSP through this RFP. All security breaches shall be treated as severity level 1. The MSP shall be responsible for all the security breaches by unrestricted access, misconfiguration, unpatched vulnerabilities, insufficient monitoring, week passwords, or any unknown factor etc. Some of the common security breach examples shall include but not limited to the following:

i. Data Loss, Data leak, Data is mined.
ii. Corruption of Data
iii. Data theft (including internal incidents)
iv. Privacy Breach
v. Loss/Missing of Logs
vi. Exfiltration of Data
vii. Phishing, spam, vishing attacks
viii. Infection of Malware, Trojan, Virus, Ransomware, Worms etc.
ix. Unauthorized access to a data, application, service, database, hardware, software, SOC premises etc.
x. Denial of service, Distributed Denial of Service
xi. Security misconfiguration
xii. Negligence/mishandling of ICT infrastructure by the MSP team.
xiii. Violation of existing security best practices and SoP defined by the Purchaser.
xiv. Any type of Sabotage

U. The MSP shall assume responsibility for compensating the Purchaser for direct and indirect damages, including but not limited to financial losses, reputational damage, legal fees, and regulatory penalties arising from the security breach.

V. Penalty calculation for security breaches will be calculated independently of the overall capping of the penalty of the RFP.

Penalty when a security breach has occurred		
Sr.No	Description	Penalty
1	No Security breaches	No Penalty
2	In case of any Security Breach as defined in Sr. no . 6 (pt. no T):	1. 5% of the quarterly payment for every breach. 2. Additional 2 % of the quarterly payment for every additional day till the security breach is resolved. The penalty for security breaches is capped at 50% of the quarterly payment.

W. All costs associated with remediation efforts, investigation, notification, customer support, credit monitoring, and any other actions deemed necessary by the contracting party to mitigate the impact of the breach shall be borne by the MSP.

X. The MSP shall also bear the responsibility for any third-party claims arising from the security breach.

Y. Any downtime within scope of this RFP resulting out of the reasons not attributable to the MSP will not be accounted for the calculation of penalty subject to production of supporting evidence by the MSP.

7 General Conditions

A. The bidder/OEM should undertake to provide support for the supplied solution for a period of 7 years (including 5-year warranty & support).

B. No deviations from these terms and conditions will be accepted. Any violation thereof will lead to rejection of the bid.

C. The decision of Supreme Court of India /NICSI arrived during the various stages of the evaluation of the bids is final & binding on all vendors. Any representation towards these shall not be entertained.

D. In case the selected bidder is found in-breach of any condition(s) of tender or supply order, at any stage during the course of supply/ installation/commissioning or warranty period, the legal action as per rules/laws, shall be initiated against the bidder and PBG shall be forfeited.

E. Any attempt by bidder to bring pressure towards decision making process, such bidders shall be disqualified for participation in the present tender.

F. Printed conditions mentioned in the tender bids submitted by bidders will not be binding on Supreme Court of India /NICSI. All the terms and conditions for the supply, testing and installation, payment terms, penalty etc. will be as those mentioned herein and no change in the terms and conditions by the vendors will be acceptable.

G. Upon verification, evaluation / assessment, if in case any information furnished by the bidder is found to be false/incorrect, their total bid shall be summarily rejected and no correspondence on the same, shall be entertained.

H. An NDA as per mutually agreed terms will be signed with the selected bidder later on.

Annexure Documents

1. Annexure : Manufacturer's Authorization Format (MAF)

Date: _____ RFP No.: _____

To,
Tender Division,
National Informatics Centre Services Inc.,
1st Floor, NBCC Tower,
15 Bhikaji Cama Place,
New Delhi -110066
Tel: 011-22900534/35

Subject: Manufacturer Authorization for participation in the RFP of NICSI titled "RFP for ICT Enablement for Supreme Court of India Data Centre" and RFP No._____.

Sir,

We, <OEM/ Manufacturer name> having our registered office at <OEM/ Manufacturer address>, are an established and reputed manufacturer of < name of quoted item >.

We confirm that <MSP Name> having its registered office at <MSP Address> is our authorized partner for <item name>. We authorize them to quote for our equipment in the above-mentioned tender.

Our full support is extended to them in all respects for supply, 5 years of warranty and maintenance of our products as per the bid terms.
We confirm that the quoted product is not end of sale (EoS) and service support will be available for a period of 7 years from date of supply/installation of the equipment irrespective of its end of service life (EoSL) timeline, provided the support renewal is active.
We also undertake that in case of default in execution of this tender by the <MSP Name>, the <OEM/Company Name> will take all necessary steps to provide service support for our equipment as per tender terms.

Thanking You

For **<OEM/ Manufacturer name>**

<(Authorized Signatory)>
Name:
Designation:
Corporate E-mail ID:
Seal of the Company

2. Annexure: Manpower/resource categories, skillset and qualifications

For the position of 'Project-in-charge', it is mandatory to provide name of proposed resource along with details desired as per format given below. **It is mandatory that the resource proposed for this position should not change till the commissioning and acceptance of the complete solution.**

For all other categories of manpower resources, the names & date of birth of proposed resources may be furnished by the Bidder at the time of contract finalization.

a) Qualification, Experience & Skillset for Resources (Minimum Requirement)

Note: The above designations are minimum and indicative in nature. The bidder shall provision adequate designations to meet the SLA. However, the bidder shall list out all the designations as per their proposed solution along with quantity.

Sr. No	Position	Key Responsibilities	Minimum Qualifications
1.	System Administrator	• Managing security, compliance & accreditation including internal and external regulations and policies • Perform server maintenance in production and non-production environments. • Supporting the service / Help Desk with day-to-day end-user assistance, incident troubleshooting and resolution, and physical IS asset re-location. • Supporting catalogue requests including accepting, approving, and fulfilling provisioning requests • Managing the maintenance of server's operating systems	• Total Experience: 5 years of relevant experience • Certification: Linux Administration
2.	Network and Security Administrator	• Experience in daily network operational tasks that would include configurations, communication performance, in a secure, reliable, and highly availability environment. • Experience in operation and support of Application Centric Infrastructure (ACI) • Familiarity with and demonstrated understanding of enterprise's business and technical architecture. • Hands-on technical knowledge of network systems, protocols, and standards such as ethernet, Wi Fi, LAN, WAN, STP, VPC, VxLAN etc.,) • Minimum of 3 years' experience working in a switched and routed environment (OSPF, BGP, MPLS, MPBGP, VPN etc.,) • Operation and support of application load balancer: F5 (LTM & GTM)	• Total Experience: 3-5 years of relevant experience • Certification: Cisco/ Juniper Professional Certification in Datacenter Networking in mandatory.
3.	Storage & back up Administrator	• Knowledge of storage and backup hardware architectures • Familiarity with high-level programming languages	• Total Experience: Minimum 5 years' experience

Sr. No	Position	Key Responsibilities	Minimum Qualifications
		• Experience working in a distributed file system environment. • Experience adding and removing disks, disk group management, logical unit numbers (LUN) management and provisioning. • Experience planning, monitoring, repairing, and reporting on storage resources. • Experience with infrastructure capacity planning. • Experience providing general IS user support. • Experienced installing and configuring SAN storage controllers. • Experience in monitoring the state of backup/recovery resources including the availability of allocated backup storage space, replication to offsite. • Experience in managing the inventory of offsite storage of backup media and ensure that backup media handling conforms to established procedures. • Familiarity with and demonstrated understanding of enterprise's business and technical architecture. • Experience in archival processes, strategies, and tools • Experience in enterprise storage management systems • Experience on large storage management initiatives • Experience working on large enterprise backup & recovery initiatives. • Extensive experience in scheduling backup operations, including job creation, scheduling, and backup completion status monitoring across all platforms	• Certification: Storage Technology Certification, Windows Server Administration, Red Hat Certified System Administrator
4.	Database Administrator (MySQL/ Postgres DB/ MS-SQL/MongoDB)	• Experience in daily database operational tasks that would include configurations, performance, backup, recovery, disaster recovery scenarios and manage data in a secure, reliable, and highly available system environment. • Knowledge of database storage infrastructure • Experience in planning, monitoring, repairing, reporting and other day-to-day tasks associated with maintaining database resources in an optimal fashion. • Experience in Infrastructure capacity planning	. • Total Experience: Minimum of 5 years' experience in IT Infrastructure domain having experience in managing large IT Projects. • Certification: Any Associate level cloud certifications from the proposed CSP is mandatory

Sr. No	Position	Key Responsibilities	Minimum Qualifications
		• Familiarity with and demonstrated understanding of enterprise's business and technical architecture	
5.	Cloud Administrator	• Configuring the cloud management service • Managing the cloud management service • Integrate cloud-based systems into the existing environment. • Resolve operational issues. • Change requests for cloud management service upgrades must be approved or denied. • Key metrics for cloud resources should be monitored. • Load balancing • New cloud computing technologies should be evaluated and implemented. • Examine summary data from cloud resource deployments	• Total Experience: The resource should have a minimum of 3 – 5 years' experience in IT Infrastructure domain. • Certification: Any Associate level cloud certifications from the proposed CSP is mandatory

Manpower deployment details:

The bidder shall propose the year wise manpower deployment in the format provided below:

Sr. No	Designation	Quantity				
		Year 1	Year 2	Year 3	Year 4	Year 5
1						
..						

Note: The no. of resources proposed for each designation shall not change during the contract period.

For <MSP>

< (Authorized Signatory)>

Name:

Designation:

Contact Details:

Seal of the Company

3. Annexure: Bidder's Blacklisting Declaration

Date: _____ RFP No.: _____

To,
Tender Division,
National Informatics Centre Services Inc.,
1st Floor, NBCC Tower,
15 Bhikaji Cama Place,
New Delhi -110066
Tel: 011-22900534/35

Subject: Declaration for bidder's blacklisting for participation in the RFP of NICSI titled "RFP for ICT Enablement for Supreme Court of India Data Centre" and RFP No._____.

Sir,

We, **<MSP>**having our registered office at **<MSP address>,** are an established authorized partner cum MSP since last **<No. of years>** and have our registered office at **< address of registered office >**.

We do here by confirm, that we have read and understood each and every tender terms and conditions of above cited tender and are bidding in complete compliance of all terms & conditions of tender. We understand that it will be our sole responsibility to deliver the product and services as per conditions set out in tender. Any failure at our end will make us liable for penalties as defined in tender and cancelation of empanelment.

We also confirm that every supply will have OEM support pack of five years for back-end support, although we will provide comprehensive warranty as per tender requirement directly. We will take all necessary steps for successful execution this project as per tender requirements.

We do hereby also confirm that our company has not been blacklisted in any Central / State Government department, public sector undertaking and autonomous body in last three years.

Thanking You

For **<MSP>**
< (Authorized Signatory)>
Name:
Designation:
Contact Details:
Seal of the Company

4. Annexure: Check list of documents to be submitted

Date: _____ RFP No.: _____

Sr. No	Description	Document Submitted (Yes / No / NA)	Reference Page no.	Remarks
1.	Submittals as per Sr.no 4.1.1 Prequalification Criteria			
2.	Submittals as per Sr.no 4.2.2 Technical Evaluation Criteria			
3.	Proposed Technical solution document against the Scope of Work of the RFP			
4.	Technical Presentation as per clause 6 of the Sr.no 4.2.2 technical Evaluation Criteria			
5.	Proof of Authorized Signatory in the form of Power of Attorney / Board Resolution			
6.	Annexure: Manufacturer's Authorization Format (MAF)			
7.	Annexure: Manpower/resource categories, skillset and qualifications			
8.	Annexure: Bidder's Blacklisting Declaration			
9.	Annexure: Bidder Particulars			
10.	Annexure: Un-priced BOQ with details of quoted products/solutions with OEMS (Signed by the Authorized Signatory)			
11.	Annexure: Technical Specification (Compliance Sheet along with proper cross referencing and data sheets)			
12.	Annexure: Warranty			
13.	Annexure: Format for Price Breakup (GTV) (to be submitted separately)			
14.	Any other relevant Documents regarding the proposed solution			

For **<Bidder's Name>**
< (Authorized Signatory)>
Name:
Designation:
Contact Details:
Seal of the Company

5. Annexure: Bidder Particulars

Date: _____ RFP No.: _____

Sl. No.	Area of the details to be provided		Responding Firm's/Company Details to be provided
1.	Name of the Bidder		
2.	Address of the Bidder		
3.	Telephone number of the Firm /company		
4.	Name of the contact person to whom all references shall be made regarding this RFP		
5.	Designation of the person to whom all references shall be made regarding this tender		
6.	Address of the person to whom all references shall be made regarding this tender		
7.	E-mail address of the Firm/company		
8.	Fax number of the Firm/company		
9.	Website address of the Firm/company		
10.	Details of Registration	1. Registration Number of the Firm/company. 2. Name of the place where the firm/ company was registered. 3. Date when the company was registered. 4.Product /Service for which registered 5. Validity Period, if applicable.	
11.	Central Service Tax No.		
12.	VAT/Service Tax No.		
13.	PAN No.		
14.	• Annual Turnover during last three financial Years last three years. • Net worth		
15.	Income Tax Paid during the last three financial Years		
16.	Details of ownership of the firm (Name and Address of the Board of Directors, Partners, etc.)		
17.	Name of the authorized Signatory who is authorized to quote in the tender and		

Sl. No.	Area of the details to be provided		Responding Firm's/Company Details to be provided
	enter into the rate contract (Power of Attorney to be submitted)		
18.	Name of the Bankers along with the branch (as appearing in MICR cheque) & Account #		
19.	Status of Firm/company like Pvt. Ltd. etc.		
20.	Locations and addresses of the offices.	1. The corporate address 2. The official address of the service delivery centers at Consignee Location	

Witness:

Signature ----------

Name ----------

Address ----------

Date ----------

Bidder:

Signature ----------

Name ----------

Designation ----------

Company Seal----------

Date ----------

6. Annexure: Site Not Ready Declaration

Date: _____ RFP No.: _____

Site Not Ready Certificate		
1	MSP Name	
2	Purchase order No. & date	
3	Location Name	
4	Equipment Name	
5	Date of delivery	
6	Date of 1st Visit for installation	
7	Site not ready reason	
8	Tentative date of site being ready for installation	

Name of Supreme Court of India / Site in charge: ……

Designation: ……

Signature (with official seal): ……

7. Annexure: Technical Specification

7.1Compute Server

Brief Specifications: 2 CPU 32 cores, Minimum of 2048 GB (32 * 64 GB DDR5 DRAM), 2 * 960 GB SSD, 2*25Gbps Dual Port NIC card, Support of DPDK and SR-IOV, etc. – 5 Yrs. Support

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
1	2 x86 based architecture or equivalent processors (of latest series), min. 32 cores with 2.2 GHz or higher base frequency per processor, TDP should be within the range of 185- 210 Watts (per processor) when operating at the base frequency		
2	Server should be configured with a Minimum of 2048 GB (32 x 64 GB DDR5 DRAM) memory		
3	2 * 960GB or more SATA SSD (must have Hardware RAID-1 in mirrored configuration with dedicated controller & hot plug bootable drives) DWPD 1 & higher.		
4	Server should be max 2 RU with 6 PCIe Gen5 free slots before configuring any Cards		
5	Management (IPMI) Port (1 x 1 Gbps) and PxE (2 x 1 Gbps)		
6	2 * 25 Gbps Dual Port network cards, the server should have card level redundancy. Server should support DPDK and SR-IOV features. DPDK on 25G card should deliver 0 packet loss as per RFC 2544 and deliver 100%-line rate for all the packet sizes over 64 Bytes. Vendor should provide necessary 25G connectivity. Vendor shall offer appropriate 10 meters LC-LC cable and 25Gig SFP for connecting these to the offered upstream Switch Ports. Vendor shall own the compatibility of the offered cable with NIC and Upstream Switch.		
7	OS Certification & Compliance: Latest and future releases of Linux (compliance certification from RedHat for RHEL, Canonical for Ubuntu). Vendors should provide documentary evidence to substantiate their compliance claims		
8	Virtualization/Cloud Platform Compliance: OpenStack & Kubernetes. Vendors should provide documentary evidence to substantiate their compliance claims		
9	Minimum 2 * 32 Gbps FC port on two different controllers with two number of 10m LC-LC Cable		
10	Server shall provide Secure Boot (Firmware and BIOS level Security)		
11	The system should be capable to stop execution of Application/ Hypervisor/ Operating System in case of any security breach		
12	Provision to lock the system in case of any security breach		
13	Hardware root of trust/dual root of trust		
14	The server should provide policy-based security		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
15	The server should provide rack server intrusion detection		
16	The server should provide cryptographic firmware updates		
17	All the products proposed should be supported by a “Malicious code free” authorization letter legally vetted by the OEM		
18	All the patch cords (fibre and copper) should be supplied with each server.		
19	The OEM should have published spec rating for the required processor		

7.2Object Storage (500 TB)

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
1	Object storage appliance should be supplied with minimum 5 nodes (Appliance Based) consisting of SSD/NVME Drives. Each object storage appliance should be configured with minimum 2 x 25 Gbps LAN ports, Redundant Load Balancer must be offered. Object Storage appliance, Load Balancer HW and Software solution must be owned and supported by single OEM.		
2	The proposed object storage solution should support mirroring and erasure coding		
3	The proposed solution should support defining the type of protection, tiering of data across available nodes/sites and geography of storage locations and set retention period		
4	The object storage cluster shall be scalable to minimum 100 PB and 100 Billion Objects in a single namespace by adding drives and nodes. The expansion of object storage should support intermixing of node types & disk sizes supporting asymmetric upgrades across sites.		
5	Clause has been removed		
6	Proposed object storage should be fully distributed, asymmetrical, and scale-out architecture allowing multi-site Active/Active architecture.		
7	For enhanced data security requirement, the solution must support data at rest encryption along with data in transit encryption capabilities based on AES-256-SHA.		
8	Offered Config must offer minimum of 15GB/sec read throughput, OEM Sizer report must be submitted duly signed and stamped by OEM on their letterhead,		
9	The proposed solution should also support tiering of data to third-party cloud		
10	Object storage must provide balancing of the stored capacity across all nodes in a cluster, ensuring, load get evenly distributed across all nodes. Load Balancer should be included as part of the solution as per throughput asked.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
11	Object storage should return the unique identity information for the stored object, which is a digital cryptographic hash algorithm along with unique version ID, storage location, date & time stamp etc		
12	Object storage nodes/controllers must have inbuilt support for S3 API should not require any third-party software or hardware or gateway to perform ingest & retrieval.		
13	Proposed object storage solution should support "indexing" and should have time base retention at the object level. Furthermore, the solution should also provide integration capabilities with external search engines.		
14	The proposed object storage solution should support object sizes from few kilobytes to 5TB. If space reclaim after deletion is impacted with small size object deletion (less than 1MB) then addon 30% Capacity must be supplied.		
15	Object should be tamperproof from outside access/intrusion and there should not be root level permission. Only remote monitoring should be available, if required.		
16	Proposed Object Storage should not allow users to access data via system-console login to the cluster's nodes and it should be used only for management.		
17	Object storage should perform online storage migration to newer system generations to handle end of life support without application downtime.		
18	Object storage should maintain the authenticity and integrity of objects using hash keys such as MDS/SHA-1/SHA-2 with self-healing and auto-configuration feature as well.		
19	Object storage should have metadata-driven policies to automate placement, protection, availability at object, tenant, custom intent either manually or from application or system levels and set retention and expiration.		
20	Object storage should be able to scale seamlessly and asymmetrically across geographically dispersed data centers without any reconfiguration of system.		
21	Object storage should be able to scale up seamlessly with zero impact to existing data availability.		
22	Offered HW and SW must be engineered for singe lifecycle and supported by one OEM for end-to-end environment. Respective must be providing firmware and hardware upgrades for end-to-end environment including storage hardware, Object Storage code and OS components		

7.3Unified Storage (500 TB)

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
1	Offered Storage must have scale-up and/or scale-out architecture for SAN and NAS protocols asked. It must also support data in place upgrades for the Storage controllers to higher generation of controllers while data is intact in old NVMe media. Storage must be offered with purpose built single operating system supporting block & file protocols .		
2	Offered Storage must support Symmetric or Asymmetric Active/Active architecture for block access, it also must support file shares to be accessible from all available controllers.		
3	Offered Storage must be supplied with 500 TiB of usable capacity after concurrent dual drive failure protection and spare drives as per OEM's best practices. Offered storage must be based on end-to-end NVMe architecture.		
4	Offered Storage must be configured with minimum of 48 Cores per Controller. Storage must be configured with minimum 512GB or more DRAM based Global/Federated Cache/Memory per controller. Writes in the cache must be protected in the event of unplanned power outage by destaging to persistent storage or battery backed cache.		
5	Offered Storage configuration must be sized to support minimum 500k IOPS with 8K 70:30 RW Random Workload along with data reduction enabled. Offered solution must support minimum 4X scalability of performance by leveraging scale up or scale out architecture. OEM Sizer report must be submitted on letterhead.		
6	Array must be offered with minimum 4x25Gbps SFP28 Ethernet ports and 8x32G FC Ports across controllers supporting asked protocols. Offered storage must also support 100 Gbps Ethernet within offered controllers and without change of the offered controllers. Dedicated Management ports must be offered.		
7	Offered Storage must support capacity scalability of 2x the usable capacity asked within offered controllers and higher capacity scalability in scale-out fashion.		
8	Offered Storage must support minimum of 250 Redirect on write snapshots per volume, Production SAN and NAS Volumes must be protected with point-in-time copies.		
9	Offered Storage must provide application consistent data protection within the datacenter (Snapshots & Thin clones) or by replicating to the remote datacenter. It must support VMware, MS SQL, Mongo DB, Oracle , SAP MaxDB, PostgreSQL, etc.		
10	The storage operating system must provide FC, NVMe-oF, NVMe/TCP, iSCSI,NFS (NFSv3, NFSv4, NFSv4.1), CIFS/SMB protocols natively to support heterogeneous application environment.		
11	Offered Storage must provide Inline as well as Post-Process deduplication, compression for both Block and File data.		
12	The storage system should offer capability to provide immutable snapshots to protect point in time copies from deletion even with Admin privileges. Array must support minimum 250 snapshots per SAN and NAS volume.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
13	Offered Storage must be configured with required Licenses to configure: Asynchronous Replication for both block and file system between 2 DCs.		
14	Offered Storage replication should be secured by end-to-end encryption and bandwidth optimization over a WAN link natively or with additional required redundant hardware. All the necessary hardware & licenses should be quoted from day 1 in Highly available configuration.		
15	The proposed storage array must support data-at-rest encryption in compliance with FIPS 140-2 certification managed by in-built Key Manager or External Key Manager.		
16	The storage should be configured to comply with SEC Rule 17a-4 for File data in order to protect the data with WORM protection.		
17	Offered Storage must have capability to implement Quality of Service which must allow administrators to limit IOPS and throughput for certain Block Luns and File shares. Required HW and SW must be offered.		
18	Storage system must be offered in a No-Single-Point of Failure offering up to six 9s of availability with scale up and scale out architecture.		
19	Offered Storage must have integration with VMware ecosystem e.g., vVOLs, VAAI, it must support Storage Policy based Management as well as NVME connected vVols. Offered Storage must support integration with OpenStack Cinder for block and OpenStack Manila for File protocols.		
20	Offered Storage must provide Latest CSI driver for providing persistent storage to K8s environments, CSI driver must be a supported by the OEM.		
21	Offered Storage must be offered with UI and CLI to configure, manage and monitor the offered storage hardware and other features. It also must have RESTFul & Ansible scripts available to configure and Manage the storage.		

7.4Archival Storage (1 PB)

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
1	Proposed object storage should be offered with minimum 1 PB of usable storage capacity. Proposed Object storage should be able to scale to petabytes of unstructured data storage and to store it over longer periods of time.		
2	Object storage appliance should be supplied with minimum 3 nodes (Appliance Based) consisting of NL-SAS Drives. Each object storage appliance should be configured with minimum 2 x 25 Gbps LAN ports, Redundant Load Balancer must be offered. Object		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
	Storage appliance, Load Balancer HW and Software solution must be owned and supported by single OEM.		
3	The proposed object storage solution should support mirroring and erasure coding.		
4	The proposed solution should support defining the type of protection, tiering of data across available nodes/sites and geography of storage locations and set retention period		
5	The object storage cluster shall be scalable to minimum 100 PB and 100 Billion Objects in a single namespace by adding drives and nodes. The expansion of object storage should support intermixing of node types & disk sizes supporting asymmetric upgrades across sites.		
6	Clause has been removed		
7	Proposed object storage should be fully distributed, asymmetrical, and scale-out architecture allowing multi-site Active/Active architecture.		
8	For enhanced data security requirement, the solution must support data at rest encryption along with data in transit encryption capabilities based on AES-256-SHA.		
9	Offered Config must offer minimum of 1.5GB/sec read throughput, OEM Sizer report must be submitted duly signed and stamped by OEM on their letterhead,		
10	The proposed solution should also support tiering of data to third-party cloud.		
11	Object storage must provide balancing of the stored capacity across all nodes in a cluster, ensuring, load get evenly distributed across all nodes. Load Balancer should be included as part of the solution as per throughput asked.		
12	Object storage should return the unique identity information for the stored object, which is a digital cryptographic hash algorithm along with unique version ID, storage location, date & time stamp etc		
13	Object storage nodes/controllers must have inbuilt support for S3 API should not require any third-party software or hardware or gateway to perform ingest & retrieval.		
14	Proposed object storage solution should support "indexing" and should have time base retention at the object level. Furthermore, the solution should also provide integration capabilities with external search engines.		
15	The proposed object storage solution should support object sizes from few kilobytes to 5TB. If space reclaim after deletion is impacted with small size object deletion (less than 1MB) then addon 30% Capacity must be supplied.		
16	Object should be tampering proof from outside access/intrusion and there should not be root level permission. Only remote monitoring should be available, if required.		
17	Proposed Object Storage should not allow users to access data via system-console login to the cluster's nodes and it should be used only for management.		
18	Object storage should perform online storage migration to newer system generations to handle end of life support without application downtime.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
19	Object storage should maintain the authenticity and integrity of objects using hash keys such as MDS/SHA-1/SHA-2 with self-healing and auto-configuration feature as well.		
20	Object storage should have metadata-driven policies to automate placement, protection, availability at object, tenant, custom intent either manually or from application or system levels and set retention and expiration.		
21	Object storage should be able to scale seamlessly and asymmetrically across geographically dispersed data centers without any reconfiguration of system.		
22	Object storage should be able to scale up seamlessly with zero impact to existing data availability.		
	Offered HW and SW must be engineered for singe lifecycle and supported by one OEM for end-to-end environment. Respective must be providing firmware and hardware upgrades for end-to-end environment including storage hardware, Object Storage code and OS components		

7.5Backup Solution (500 TB)

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
A	**Hardware**		
1.	**Capacity:** Proposed purpose-built backup appliance (PBBA) should be sized appropriately for backup of **front-end data of 500TB** (30% DB, 70% File System) as per below mentioned retention policies: a) Daily Incremental Backup – retained for 21 days. b) Weekly Full Backup for all data types – retained for 28 days. **Scalability:** The appliance should be quoted with adequate provision for future capacity expansion of minimum **1 PB front end data**. Any additional software / other component required as per sizing needs to be provided by the OEM & bidder at the time of bid. The bidder must also submit the backup capacity sizing certificate/report on the OEM's letter head with seal and sign from authorized signatory.		
2.	Proposed appliance should be able to interface with various industry leading server platforms, operating systems and must support LAN/SAN based backup via NFS v3, CIFS, FC and NDMP protocols. All of the protocols should be available to use concurrently with global deduplication for data ingested across all of them.		
3.	Proposed appliance should support global and inline data duplication.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
4.	Proposed appliance should support tight integration with quoted backup software and should support source side deduplication (at host level) so that only changed blocks travel through network from source host to backup device.		
5.	Proposed solution should support different retentions for primary and DR backup appliance with support for transmitting only deduplicated unique data in encrypted format to remote sites.		
6.	Proposed appliance should support retention lock feature which ensures that no data is deleted accidently or deliberately. Even Administrator should not be able to delete the data deliberately & accidently till the retention of the backup get expired. In case this data is replicated to DR/Secondary site, no additional licenses must be required at DR site to maintain retention lock on replicated data.		
7.	Proposed appliance should be offered with battery backed up NVRAM for protection against data loss in power failure scenario and continuous automated file system check to ensure data integrity.		
8.	Proposed appliance should support 128/256-bit AES encryption for data at rest and data-in-flight during replication. It should offer internal and external key management for encryption.		
9.	Proposed appliance should be offered with Multi-Tenancy features which provides a separate logical space for each tenant user while maintaining a global deduplication across data from all tenant users.		
10.	Backup solution should have security feature which ensures that even administrator is not able to delete the backup data deliberately or accidently till the retention period of the backup data is expired in purpose built backup appliance. The security feature should also protect against NTP hacking/compromise. In case this backup data is replicated to DR/Secondary site, no additional licenses must be required at DR site to maintain retention period on replicated data.		
11.	The backup solution should support for ease of user rights management along with role-based access control to regulate the level of management in multi-tenant environment		
12.	The proposed backup software should have the capability to enable WORM on the backup sets from the backup software console on proposed purpose-built backup appliance. The implementation should ensure that no data can be deleted on the backup appliance even by the administrator deliberately or accidentally.		
13.	Proposed backup software should be available on various OS platforms like Windows, Linux, HP-UX, IBM AIX, Solaris etc. The backup server should be compatible to run on both Windows and Linux OS platforms.		
14.	The proposed backup software should support restore a single VM, single file from a VM, a VMDK restore from the same management console for ease of use.		
15.	The proposed backup solution should have in-built feature for extensive alerting and reporting with pre-configured and customizable formats. The proposed solution must have capability to do trend analysis for capacity planning of backup environment not limiting to Backup Application/Clients, Virtual Environment, Replication etc.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
16.	The proposed backup software should have the capability for block-based backups with granular recovery capability for Windows, Linux, Hyper-V, VMWARE and Exchange for faster backups on supported Disk platforms.		
17.	The proposed backup solution should provide search capability from a web portal to allow search for a single file from complete backup store.		
18.	The proposed PBBA must integrate with the proposed backup software to support backup and recovery of OpenStack virtual machines running on Ceph RBD and Cinder disk attachments. The solution must communicate with OpenStack APIs such as Nova and Glance to collect metadata and for the import of the restored process. The solution should also support integration with Hyper-V, ESXI and Kubernetes.		
19.	The proposed backup solution should support completing backup of 1 PB within a backup window of 12 hours.		
B	**Software**		
20.	Backup software should support Agentless deployment of backup software for Virtual machine and volume backup		
21.	Integrates in Cloud platform for Tenant self-service		
22.	Supports application awareness		
23.	Protects VMs and volumes		
24.	Tenants can recover single files from backups		
25.	Supports need for full workload restore to other Tenants/Clouds for test/dev refresh		
26.	Multi tenancy support		
27.	Backup scheduler		
28.	Supports workload re-configuration		
29.	Support for backup of boot and data volumes (boot and data) for VMs		
30.	Backups can be restored at second site		
31.	Backups can be full or incremental		
32.	Can roll through a full retention period		
33.	Role based permissions		
34.	should report on Tenant backup usage		
35.	should report on backup job status		
36.	Report on Backup trending by tenant		
37.	Backup software should support backup for VMs running in Hyper-V, VMware and OpenStack		
38.	Backup software should provide online backup for MS-SQL, Oracle RAC, MySQL, Postgres-SQL, mongo dB etc. on different platforms like Windows / Unix / Linux etc.		
39.	Helm or Package deployment		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
40.	Infinite Scale		
41.	Integration with Dashboard with Role-based actions and self-service		
42.	Support for Kubernetes Objects like: etc (cluster database), state file (cluster configuration), cluster configuration file (cluster configuration), certificates (cluster configuration), persistent storage (stateful apps), containers (images used by apps), cluster configs		
43.	Support for backup and restore part of a cluster by using namespaces or label selectors.		
44.	Support for pre- or post-backup hooks for custom actions		
45.	Redeployment Method: Manual, Scripted, Automated		
46.	Supports application awareness		
47.	Protects Configuration and PVCs		
48.	Supports need for full workload restore to other Tenants/Clouds for test/dev refresh		
49.	Aware of tenant boundaries		
50.	Backup scheduler		
51.	Support for restore when Infrastructure or Hardware Failure		
52.	Policy-based backup automation and monitoring		
53.	Support to restore in case of Application Misconfiguration		
54.	Support for Accidental or Malicious Data Loss		
55.	Unified backup catalogue /architecture		
56.	Supports workload re-configuration		
57.	Backups can be restored at second site		
58.	Backups can be full or incremental		
59.	Can roll through a full retention period		
60.	Role based permissions		
61.	Can report on Tenant backup usage		
62.	Can report on backup job status		
63.	Report on what applications is covered vs not covered by workloads		
64.	Backup trending by tenant		
65.	Bidder should offer solution to ensure backup and restore every tenant cluster, namespaces , and even groups of resources using Kubernetes label selectors. It can also backup across clouds or move K8s workloads with cross-cluster restore.		

7.6Spine Switch

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
1	Should be 1RU to 12U based configuration having 32x 100G QSFP ports populated with 24x 100G BD SFP's . Switch should have support for minimum 4* 400G ports also. Quoted switch should be upgradable to 48x 100G QSFP ports.		
2	Transceivers should be from Same OEM of Switch.		
3	Non-blocking architecture and Wire rate L2 & L3 forwarding. Throughput: 6400 Gbps and 2000 Mpps		
4	Should have Redundant hot-swappable Fans & power supplies. Should have USB and console ports.		
5	Should have x86 based multicore processor with minimum 8GB of RAM onboard		
6	Switch should have modular operating system with ability to contain faults and repair/restart process state fully. Should have support for ISSU/fast upgrade or live patching.		
7	Should support 224K MAC address, 256K IPv4 prefix Routes, 4096 802.1Q VLANs		
8	Should Support telnet, industry standard CLI, SSHv2, HTTPS, SCP, SFTP, NTP, DHCP server, PTP, SNMP v1/2/3, LLDP.		
9	Should support AAA, TACACS+, Radius; MAC,IP and Port filter support in ACL; storm control, Control plane protection from DoS.		
10	Should support QoS, COS/DSCP trust, 802.3x, PFC, ECN, priority Queuing, 8 queues per port, ACL based classification, 9200 bytes jumbo frame, policing and shaping.		
11	Should have automation support with python, bash, API, ansible, dockers and zero touch provisioning for custom programmability and use cases.		
12	Should have advance mechanisms for in-depth troubleshooting and monitoring like packet capture on the device, port mirroring, filter session through SPAN (VLAN/ACL), real time streaming telemetry, microburst congestion detection and reporting, TWAMP, sFlow/Netflow.		
13	Should support MSTP, per VLAN RSTP, LACP, 802.1q trunking, Static routing, OSPFv2 and OSPFv3, ISISv4 and v6, RIP, PIM-SM, BGP, VRF, Anycast-RP, VRRPv4 and v6, IGMP, BFD, 64- way ECMP and PBR on day-1 with software ready support for advance protocols VXLAN+EVPN and segment routing if required in future.		
14	Should have Common Criteria (ISO/IEC 15408) EAL or NIAP/CCEVS or NDPP/NDcPP certification for the model or family or solution		
15	Hardware and TAC support should be directly from the OEM. OEM should have 24x7 TAC supported. For genuine parts replacement and proper maintenance of records for warranty, RMA should be processed directly by the OEM only. OEM email-id and India Contact support no. to be provided.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
16	Device should support same OS image as other devices within the fabric for simplified operations and management.		
17	Device should have IPv6 ready with IPv4 and IPv6 dual stack support		
18	0 to 40-degree Celsius operating temperature, 19" rack mountable with front to back airflow.		
19	All licenses should be provided with the devices for the mentioned features.		
20	Visibility: Should integrate events from all devices as part of the RFP and should be able to show in a Single Pane of Glass View - Dashboard to manage services and infrastructure. Tool should provide end to end view of network health into a consolidated, central console with customizable dashboard with widgets and allow to provide monitoring of different metrics and End-to-end visibility of network & alerts automatic and continuous to detect real time changes in the network and able to generate a representation of the network topology. Solution should support configuration tasks for updates, changes and configuration upload and download, compare configuration, bulk configurations and configuration backup.The Solution should have plugin-based network configuration management. The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real time; in order to keep the topology always up to date and provide a Unified Fault, Availability and Performance function from a single station only to reduce network and device loads with unified fault & performance monitoring. Solution should support deployments on industry-leading platforms like Baremetal/Vmware/ KVM/Hyper-V /etc. Hardware required for deployment of this solution need to factor by SI from Day 1. All licenses should be perpetual/subscription based in nature. In case the license is subscription based, the validity of the license should be 60 months. "Visibility software should be from same Switch OEM" or "if 3rd Party Visibility Software is quoted then Visibility software must be CMMI 3 certified and the certificate should be trackable on CMMI pars portal and must have security certification for OWASP top 10 vulnerabilities assessment by CERT-IN empanelled govt. agency".		
21	Device should be IPv6 Certified/IPv6 logo ready		
22	Device/Solution shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or EN 61000-3-3 Standards for Safety requirements of Information Technology Equipment.		
23	The Device should be EAL 3/NDPP/NDcPP certified under Common Criteria.		
24	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided. The Switching System shall be quoted with 5 years OEM Hardware warranty along with OEM web based / telephonic technical Support. The same shall be verifiable on OEMs website. All asked feature license should be supplied from Day 1 and all licenses should be Perpetual/Subscription based in nature. Hardware & Software Support 60 months. In case the license is subscription based, the validity of the license should be of 66 months.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
25	OEM & Bidder shouldn't be from a country which shares a land border with India and Hardware shouldn't be Manufactured & Assembled from a country which shares a land border with India. Same should be declared in MAF.		
26	All Network Switches should from Same OEM, for better support and no compatibility issue come up at later stage		
27	All Network Switches should run on same OS for simplified operations.		

7.7Leaf Switch

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
1	The Switch should support line rate & 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 level of redundancy and must be hot swappable.		
3	Switch and optics must be from the same OEM		
4	Switch should support the complete STACK of IP V4 and IP V6 services.		
5	Switch should have the following interfaces:		
6	Minimum 48 ports support 1/10/25 Gbps SFP ports for host connectivity and minimum 6*100G ports for Fabric/Spine connectivity. The proposed switch should support native 10/25G and should be populated with 46*10G/25G Multimode fiber transceivers and 2*10G Base T transceiver for downlink connectivity &6*100G ports with multimode for uplink connectivity		
7	b. 12 * 100GbE QSFP ports populated with 2*100G 5 Meter DAC cable and 4* 100G BD SFP's		
8	Switch should support IEEE Link Aggregation for redundancy across two switches in active- active mode		
9	The switch should support 128k IPv4 routes or above		
10	The switch should support hardware-based load balancing at wire speed using LACP and multi chassis ether channel/LAG		
11	Switch should support minimum 4.8 Tbps of throughput capacity		
12	Switch should support minimum 220,000 no. of MAC addresses		
13	Switch should support Jumbo Frames up to 9K Bytes on all Ports		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
14	Support storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities		
15	Switch should support Policy Based Routing		
16	Switch should provide multicast traffic reachable using:		
17	a. PIM-SM		
18	b. PIM-SSM		
19	d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)		
20	e. IGMP V.2 and V.3		
21	Switch should support Multicast routing		
22	Switch should support for BFD For Fast Failure Detection		
23	Switch should support VXLAN with EVPN control plane		
24	Switch must support symmetric VXLAN integrated routing and bridging with EVPN active- active multihoming support.		
25	Should support 8 queues per port, priority queuing, round-robin queuing		
26	Should support QoS classification, policing and shaping, DSCP and COS.		
27	Should support WRED, Explicit Congestion Notification, priority flow control, data center bridging.		
28	Switch should support control plane i.e., processor and memory Protection from unnecessary or DoS traffic by control plane protection policy		
29	Switch should support for external database for AAA using:		
30	a. TACACS+		
31	b. RADIUS		
32	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined		
33	Switch should support MAC ACLs		
34	Should support Standard & Extended ACLs using L2, L3 and L4 fields		
35	Switch should support minimum IEEE 1588 PTP boundary clock mode		
36	Should support telnet, ssh, https, SNMPv3, TWAMP, event manager, scheduler and configuration rollback for ease of operations and management		
37	Device should support on-device execution of python script, bash script and docker containers for automation and programmability support		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
38	Switch should support onboard Packet Capture using Wireshark/ tcpdump in real time for traffic analysis and fault finding		
39	All relevant licenses for all the above features and scale should be quoted along with switch		
40	Should have hot swappable and field replaceable internal redundant power supply and FAN from day one, should be provided with AC power supply and India power cords.		
41	All licenses should be provided with the devices for the mentioned features.		
42	Visibility: Should integrate events from all devices as part of the RFP and should be able to show in a Single Pane of Glass View - Dashboard to manage services and infrastructure. Tool should provide end to end view of network health into a consolidated, central console with customizable dashboard with widgets and allow to provide monitoring of different metrics and End-to-end visibility of network & alerts automatic and continuous to. detect real time changes in the network and able to generate a representation of the network topology. Solution should support configuration tasks for updates, changes and configuration upload and download, compare configuration, bulk configurations and configuration backup. The Solution should have plugin-based network configuration management. The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real time; in order to keep the topology always up to date and provide a Unified Fault, Availability and Performance function from a single station only to reduce network and device loads with unified fault & performance monitoring. Solution should support deployments on industry-leading platforms like Baremetal/Vmware/ KVM/ Hyper-V, etc. Hardware required for deployment of this solution need to factor by SI from Day 1. All licenses should be perpetual/subscription based in nature. Incase the license is subscription based the validity of the license should of 60 months ."Visibility software should be from same Switch OEM" or "if 3rd Party Visibility Software is quoted then Visibility software must be CMMI 3 certified and the certificate should be trackable on CMMI pars portal and must have security certification for OWASP top 10 vulnerabilities assessment by CERT-IN empanelled govt. agency".		
43	Device should be IPv6 Certified/IPv6 logo ready		
44	Device shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or EN 61000-3-3 Standards for Safety requirements of Information Technology Equipment.		
45	Should have Common Criteria (ISO/IEC 15408) EAL or NIAP/CCEVS or NDPP/NDcPP certification for the model or family or solution		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
46	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided. The Switching System shall be quoted with 5 years OEM Hardware warranty along with OEM web based / telephonic technical Support. The same shall be verifiable on OEMs website. All asked feature license should be supplied from Day 1 and all licenses should be Perpetual/subscription based in nature. Hardware & Software Support 60 months. In case the license is subscription based, the validity of the license should be of 66 months.		
47	OEM & Bidder shouldn't be from a country which shares a land border with India and Hardware shouldn't be Manufactured & Assembled from a country which shares a land border with India. Same should be declared in MAF.		
48	All Network Switches should from Same OEM, for better support and no compatibility issue come up at later stage		
49	All Network Switches should run on same OS for simplified operations.		

7.8Out of Band Switch / Out of Band aggregator switch

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
	Hardware platform and architecture		
1	Switch should have 48 x 10/100/1000M ports and minimum 4 numbers of 10G Fiber ports populated with 10G MM SFP		
2	Switch should support non-blocking wire rate L2 and L3 forwarding and switch should have minimum throughput of 176 Gbps		
	High Availability		
3	Shall support modern modular operating system supporting fault isolation with stateful repair and live patching.		
4	Switch should support redundant Power Supply and redundant Fans		
	L2 and L3 features		
5	Switch should support 32 K mac address, MSTP, per vlan RSTP, LLDP, LACP and private-vlan		
6	Switch should support Layer-2 interface, SVI and L3 sub-interfaces		
7	Should support 9K Bytes jumbo frames		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
8	Switch should support static routing, dynamic routing with ISIS, OSPF and BGP, VRRPv3 and VRF		
9	Switch should support Bidirectional forwarding detection, unicast-RPF, policy-based routing and GRE		
10	should support latest IETF open standard for VXLAN+EVPN with support for routed multicast, multihoming, distributed anycast gateway and symmetric routing.		
11	should support PIM-SM, PIM-BiDir and anycast-RP		
12	Should support up to 12K IPv4 routes		
13	Should support up to 4K IPv6 routes.		
	QoS and Security		
14	Device should support port ACL to filter traffic based on L2, L3 and L4 parameters		
15	Switch should support root guard, loop guard and bridge assurance		
16	The switch should support IEEE 802.1x providing user authentication, authorization, dynamic vlan assignment, dynamic ACL and CoA.		
17	Should support control plane policing to protect from denial-of-service attacks		
18	Should support role-based access control with TACACS+ and Radius		
19	Switch should support Standard 802.1p CoS field classification, Differentiated services code point (DSCP) field classification and ACL based classification		
20	Switch should support policing, shaping and Marking. Minimum 8 queues per port.		
21	Switch should support Priority flow control, explicit congestion notification and priority queuing.		
22	Clause has been removed		
	Management, Automation and Visibility		
23	Should support SNMPv3, SSH, SFTP, SCP for secure management and file transfer		
24	Should support Configuration session and rollbacks, schedular and Event Manager		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
25	Should support open standard for remote programmability using OpenConfig over gRPC/ Rest API and ansible.		
26	should support real time streaming telemetry that can be exported to external NMS like ELK, Prometheus, etc platforms.		
27	Should support onboard programmability with python and bash. Should support docker container to run third party/custom applications for monitoring and management flexibility.		
28	Switch should support remote port mirroring over GRE, ACL filtered mirroring session and onboard packet capture tool for troubleshooting and traffic analytics.		
	Support and Compliance		
29	should be certified for NDcPP common criteria EN61000-3-2/EN61000-3-3, EN 55035, IEC/EN62368-1, RoHS		
30	should support IPv4 and IPv6 dual stack simultaneously		
31	should have IPv6 ready logo certification		
32	Hardware and TAC support should be directly from the OEM. OEM should have 24x7 TAC supported. OEM email-id and India Contact support no. to be provided.		
33	Transceivers should be from Same OEM as of Device.		
34	Clause has been removed		
35	Device should support real time data collection with sflow/netflow.		
	Automation & Visibility		
36	Device should support multi-OEM hypervisor environment and should be able to sense movement of VM and configure network automatically		
37	Clause has been removed		
38	Clause has been removed		
39	Should support measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using Two-Way Active Measurement Protocol (TWAMP) as per RFC 5357		
40	should have programmability and automation support with on board python, bash and docker containers.		
	QOS		
41	should support 8 queues per port		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
42	should support priority queue		
43	should support Weighted Fair Queue or Weighted round robin or equivalent		
44	should support WRED and DSCP for CPU generated traffic		
45	should support ACL based classification for QoS		
46	Clause has been removed		
47	Should support rate limiting function like policing and shaping		
	Others		
48	should be certified for NDcPP/EAL common criteria		
49	should have IPv6 ready logo certification		
50	should be 19" rack mountable with 4-post rail mount kit provided for easy installation		
51	All licenses should be provided with the devices for the mentioned features.		
52	Clause has been removed		
53	Device should be IPv6 Certified/IPv6 logo ready		
54	Device shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or EN 61000-3-3 Standards for Safety requirements of Information Technology Equipment.		
55	The Device should be EAL 3/NDPP/NDcPP certified under Common Criteria.		
56	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided. The Switching System shall be quoted with 5 years OEM Hardware warranty along with OEM web based / telephonic technical Support. The same shall be verifiable on OEMs website. All asked feature license should be supplied from Day 1 and all licenses should be Perpetual/subscription based in nature. Hardware & Software Support 60 months. In case the license is subscription based the validity shall be 66 months		
57	OEM & Bidder shouldn't be from a country which shares a land border with India and Hardware shouldn't be Manufactured & Assembled from a country which shares a land border with India. Same should be declared in MAF.		
58	All Network Switches should from Same OEM, for better support and no compatibility issue come up at later stage		
59	Clause has been removed		

7.9SDN/Fabric Controller

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
1	The Data Center Network Manager must be capable to provide latest network virtualisation technologies to provide seamless movement of any type of user across the fabric.		
2	All inter device and uplink connectivity should be over the latest 100G or higher better connectivity for best performance.		
3	Data Center Network Manager must have fully distributed architecture without any centralised data plane, control plane and management plane processing on single device.		
4	Data Center Network Manager must be fully resilient in all aspects. It must continue to perform packet forwarding on any single link failure. A single switch failure should not impact forwarding for hosts connected to other switches. The architecture should provide two or more equal cost forwarding paths from switches to core.		
5	Management and monitoring of the Data Center Network Manager must be provided through single pane of glass for all the devices in the network.		
6	Network Devices should be auto discovered with quick deployment options minimising human effort and human errors with network wide configuration deployment.		
7	The solution should provide real time monitoring of various parameter of the network using real time state streaming telemetry or better technology.		
8	The streaming telemetry data should be available for historical analysis of past events in time-series format for 2 or more months.		
9	The solution is expected to provide real time monitoring of various parameters like CPU, Memory, interface stats (traffic counter, error, discard), MAC table, ARP table, IPv6 ND table, RIB, BGP, capacity parameters (TCAM), VXLAN, running config, traffic flow (sflow/IPFIX/Netflow), LLDP, buffer utilization per interface, MLAG Stats, Switch environment stats(FAN, Temperature, Power Supply), etc with streaming telemetry.		
10	The solution should have capability for automated topology discovery		
11	Data Center Network Manager should be capable to show in real time congestion hotspots in the network with buffer level utilization info from the network devices.		
12	Notification and events should be available to operator in a manner that are easy to corelate by directly showing them over physical topology for various device and link level metrics.		
13	The solution should support user definable work flows to carry out multiple network-wide changes with Support for execution and conditional checks.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
14	The Data Center Network Manager should have centralised dashboard to upgrade the entire fabric with ease without incurring traffic downtime in fabric core.		
15	The Data Center Network Manager should provide simplified and quick way of network wide rollback for device configuration and images to revert back changes if required.		
16	All devices in Data Center Network Manager including Core/Spine & TOR/Leaf switches, Border Leaf Switches should be able to run on single OS image for simplified operations with minimal security exposure.		
17	Data Center Network Manager/controller should not be part of the data plane and a network device must continue to forward packet in case it loses connectivity to the manager.		
18	All the hardware, software and licenses must be included as part of the solution as per the required specification.		
19	Anything extra (e.g., transceiver, fiber cables, etc) required to setup the Data Center Network Manager as per requirement has to be provided by the bidder without any extra cost.		
20	TAC support for solution must be directly from single OEM. OEM should have 24x7 TAC available over email and Phone.		
21	All licences should be provided with the devices for the mentioned features.		
22	Visibility & Automation: All Network switches & Data Center Network Manager should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution from the same OEM. Should support telemetry with time-series database view, traffic flow analytics, PSIRT/BUG visibility, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts. SI will factor required VM's to install the software in HA cluster, if any OEM wants to supply their Appliance, they allowed to in HA Cluster.		
23	Fabric must integrate with different virtual machine managers and manage network virtualization from a self-service solution via Fabric Controller/SDN Controller		

7.10 Router

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
	Hardware and Performance		
1.	Should be fixed 1RU to 5U based configuration to support at least 20*1/10GbE SFP+ Ports populated with 12*10G LR SFP,4*10G SR SFP, 2*1G LH/LX & 2*1G RJ45 and should have		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
	minimum 4* 40/100G uplink ports populated with 2* 100G LR/LR4 & 2* 100G SR4 SFP's. All ports should be Layer 3 ports by default		
2.	Must have hot-swapable redundant power supplies(1+1) and fans(N+1)		
3.	Should support minimum throughput of 350 Gbps		
4.	Shall support modern modular operating system designed for scalability and reliability and should support auto process recovery from failures		
5.	Clause has been removed		
6.	Clause has been removed		
7.	Clause has been removed		
8.	Should support LLDP		
9.	Must have routing protocols like BGP, MP-BGP, RIPv2, OSPFv3 , ISISv4,BFD , PIM, SSM, Policy based routing, Selective route download, VXLAN EVPN, VRF		
10.	Should support minimum 500K IPv4/IPv6 routes		
11.	Should support VRRP, Should support active-active port channelling mechanism.		
12.	**Security**		
13.	Clause has been removed		
14.	Should support IPv4/IPv6 and MAC based ACL		
15.	Should support Ingress ACL Scale of 2K or better.		
16.	Should support real time data collection with sflow/netflow.		
17.	**QoS features**		
18.	Should support 8 queues per port		
19.	Should support QoS classification and policing		
20.	Should support priority queuing, DSCP, traffic shaping		
21.	Clause has been removed		
22.	Should support IEEE 1588/NTP		
23.	**Management and Troubleshooting**		
24.	Should support telnet, ssh, https, SNMPv3, configuration rollback feature for ease of management		
25.	Device Should support RSVP-TE, BGP-LU, BGP-LS, auto-bandwidth, split-tunnelling, SR-TE, TI-LFA, BGP-SR, BGP-LU		
26.	Should support port mirroring based on Inbound & outbound, mirroring based on ports.		
27.	Should provide with all software license from day-1 as per RFP specification		
28.	Should support real time telemetry from Day 1		
29.	Should comply to following certifications: EN61000-3-2/EN61000-3-3, EN 55035, IEC/EN62368-1, RoHS		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
30.	All licences should be provided with the devices for the mentioned features. The licences should be perpetual in nature of should be provided or 7yr on day-1 in case of subscription-based licencing. Hardware warranty 60 months.		
31.	Router should have support for LDP, MP-BGP, L3VPN, EVPN and L2-EVPN		
32.	EVPN should be supported with MPLS and VXLAN for layer-2 and layer-3 VPN services.		
33.	should have support symmetric and asymmetric Integrated Routed and Bridging with MPLS and VXLAN		
34.	Should support TI-LFA with ISIS		
35.	Should have support for SR-TE and BGP-LU		
36.	Router shall support 6PE and 6VPE mode for IPV6 transport over IPV4		
37.	Should support VRFs over MPLS and VXLAN transport.		
38.	All the licenses for mentioned protocol support and scale to be provided as per the specification.		
39.	**QoS and Security Features**		
40.	The Device should have 8 egress queues per port and support for strict priority queuing for differentiated QoS treatment for voice, video and other type of traffic.		
41.	The Device should support 802.1p CoS and DSCP classification, ACL based classification, VLAN based classification.		
42.	Weighted round robin (WRR) / Weighted fair queuing (WFQ) or equivalent		
43.	should support traffic Policing / Shaping		
44.	Clause has been removed		
45.	should support Ingress and Egress ACLs using L2, L3, L4 fields		
46.	Should support Ingress ACL Scale of 2K or better.		
47.	Should support Service ACLs to restrict traffic for management telnet, SNMP, etc.		
48.	Clause has been removed		
49.	Should have configurable control plane (CPU) protection mechanism as a safeguard from DoS attacks.		
50.	**Management Features**		
51.	Configuration through the CLI, console, Telnet, SSH.		
52.	SNMP v1/2/3 support, NTP, Syslog		
53.	AAA support for Router management with RBAC and privileged login		
54.	TACACS+ and RADIUS for AAA		
55.	sFlow or similar open standard to support traffic analysis		
56.	Device should support IEEE 1588 PTP/NTP for advance timing/clock support.		
57.	Management over IPv6 should be supported		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
58.	device should have modular operating system with ability to contain faults and repair/restart process state fully.		
59.	Device should support real time streaming telemetry.		
60.	Should support SCP, SFTP, NTP		
61.	should support TWAMP/BFD or equivalent open IETF standard for link/host monitoring.		
62.	Device should support API for configuration and monitoring for custom requirements		
63.	Router Operating System should support SDK/ API for writing custom programs for automation		
64.	should support Open Standard including REST API and Ansible		
65.	should support configuration checkpoint and rollback.		
66.	Device should have inbuilt support for python and bash.		
67.	Device should support docker container for custom application deployment for custom monitoring and management use cases. Should have support for devOp tools like ansible/Chef/Puppet.		
68.	Clause has been removed		
69.	Clause has been removed		
70.	Clause has been removed		
71.	Clause has been removed		
72.	Device should have zero touch provisioning support.		
73.	Should have support to view historical route and mac table changes for troubleshooting purpose.		
74.	**Other**		
75.	Hardware and TAC support should be quoted directly from the OEM. OEM should have 24x7 TAC support.		
76.	Should be NDcPP/EAL common criteria certified.		
77.	Compliance: EN61000-3-2/EN61000-3-3, EN 55035, IEC/EN62368-1, RoHS		
78.	Operating temperature of 0°C to 40°C		
79.	Manufacturer Authorization is Required		
80.	All licenses should be provided with the devices for the mentioned features.		
81.	The proposed SDWAN Solution should be implemented as true software defined WAN solution. The proposed solution should have separate Centralized Network Orchestrator, Manager and a controller along with compatible head end and Branch devices. • Management Engine- Shall be a separate component that provides single point of entry for Configuration and Monitoring. Shall be securely accessed and capable of configuration policies, monitoring and troubleshooting of multiple WAN Edge devices in the branches, data-centers or remote locations. This management engine shall be available in either physical/virtual form factor and should provide high availability.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
	• Controller - shall be a separate component that abstracts all the routing information from the edge devices and distributes route prefixes, encryption key to all Edges. The controller shall maintain centralized routing table, controls route advertisement as per policy, creates end to end segments on network, instructs data plane to change traffic flow as per the defined policy. Controller shall be available in either physical/virtual form factor and should provide Active-Active instances across DC and DR. • Orchestrator/Authentication Gateway shall be used to authenticate the onboarding edge devices using Certificates and serial number of the edge devices.		
82.	Device should be IPv6 Certified/IPv6 logo ready		
83.	Device shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or EN 61000-3-3 Standards for Safety requirements of Information Technology Equipment.		
84.	The Device should be EAL 3/NDPP/NDcPP certified under Common Criteria.		
85.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided. The router and switches shall be quoted with 5 years OEM Hardware warranty along with OEM web based / telephonic technical Support. The same shall be verifiable on OEMs website. All asked feature license should be supplied from Day 1 and all licenses should be Perpetual in nature. Hardware & Software Support 60 months.		
86.	OEM & Bidder shouldn't be from a country which shares a land border with India and Hardware shouldn't be Manufactured & Assembled from a country which shares a land border with India. Same should be declared in MAF.		
87.	All Network devices should from Same OEM, for better support and no compatibility issue come up at later stage		
88.	Clause has been removed		

7.11 Network Operation appliance

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
1	The Network Operations solution should be provided as dedicated Hardware appliance or Virtual appliance (should be hosted on a dedicated server with redundant power supply).		
2	The Hardware appliance or dedicated hardware for virtual appliance should provide redundant power supply, 2 x 10G Network Interface or better, multicore CPU and sufficient RAM and Storage to accommodate the Network Operations of entire Network Fabric.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
3	The Solution must provide the capability to create and show a graphical representation of all Network Elements in the design.		
4	The Solution must be able to interface through open APIs with external ticketing systems or centralized alerting NMS systems as used in a NOC.		
5	The Solution must provide the capability to search endpoint on the network using MAC / IP / Subnets.		
6	The Solution must integrate with 3rd-party systems through open APIs for additional reporting, with the minimum of time series databases and graphing applications.		
7	The Solution should support flow analytics (Netflow/sFlow/IPFIX) for visibility into traffic usage by endpoints.		
8	Solution should provide flow analytics using hop by hop latency and packet drop info for specific flows with reason of drop, which helps identify, locate and root-cause data path issues across fabric architecture.		
9	Solution must provide deeper visibility into the fabric in terms of latency and packet drop between any two endpoints on the fabric		
10	Solution should provide capability to proactively monitor network health over time by using time-synced data across multiple parameters to derive deeper understanding of issues and behaviours, consequently, should help in knowing the impacted endpoints, applications, and flows due to network anomalies		
11	Solution should help to track per-hop information and behaviour. It should also help to verify software and hardware programming consistency across all available traffic paths between source and destination endpoints.		
12	Solution should be able to help in the Day-2 Operation that involves root cause analysis by providing below features: a- Locate virtual machines, bare-metal hosts, and other endpoints across the entire fabric. b- Gather sequence of events from past data and provide intelligent insights. c-Provide automated root-cause analysis of data-plane anomalies, such as packet drops, latency, workload movements, routing issues, ACL drops, and more by leveraging Flow Telemetry /Flow-Telemetry Events. d- Avoid network disruption when changing configurations by predicting the impact of the intended changes before deploying. e- Provide efficient capacity planning to maintain top network performance and provide fabric-wide visibility of resource utilization and historical trends.		
13	The Solution should provide information of major bugs and field notices, also it should provide the details to stay secure and prevent unscheduled downtime.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
14	Solution should help to ensure establishing golden configuration and communication rules , and providing adherence to IT governance and security policies in the network.		
15	The Solution should provide the advanced reporting capabilities like exporting the anomaly and advisory summaries through email and PDFs/excel, provide email alerts or notification. The solution should also provide capability to export and store flow-telemetry JSONs in external storage/servers for audit purpose.		

7.12 Next Generation Firewall

Sr.No.	Minimum Technical Specifications	Compliance (Yes/No)	Cross Reference
1	Solution should be purpose build hardware appliance with Access & Threat prevention controls.		
2	The OEM shall provide 365x7x24 days technical support.		
3	All the components of the solution shall be from the same OEM		
4	The appliance should not have any active internal or external Wi-Fi component.		
5	**Specification**		
6	The proposed firewall solution shall run on a hardened OS and delivered on purposeful built hardware and security appliance.		
7	Firewall Appliances shall be rack mountable and rack mount kit shall be supplied along.		
8	Solution shall provide features and licenses for contractual period for Firewall, IPS, Site to Site VPN, Granular Application control, Anti-Malware, IPS, URL filtering/Web Security, DNS Security, Identity Awareness, VPN for 500 Users and Anti-Bot on same appliance managed through a centralized management console.		
9	Solution shall support Application level and “Stateful” policy inspection technology to prevent traffic leakage. It shall also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, http, web 2.0 application etc.		
10	The proposed security platform shall be supplied, installed, and configured in N+1 redundancy.		
11	Firewall Appliance shall provide high availability in Active- Active/Active-Passive mode. Appliance failover shall be completely stateful in nature without any manual intervention and should be completely transparent to end-user without any session drops.		
12	Appliance shall not require any downtime/ reboot for failover & backup purpose.		
13	Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public web sites		
14	It shall be possible to centrally manage Firewall and all the associated modules/ functionalities/ services over secure channel.		
15	solution shall be supplied with the support for static and dynamic routing protocols.		
16	The solution shall support VLAN tagging (IEEE 802.1q).		

Sr.No.	Minimum Technical Specifications	Compliance (Yes/No)	Cross Reference
17	Solution shall have inbuilt integration with Identity Awareness Capabilities without any external devices. Integration shall work with/without any agent on the remote side.		
18	Solution shall support Application awareness and granular control functionalities for all the commonly available Web 2.0 applications and tools.		
19	Solution shall support Link aggregation functionality (LACP/PAGP) to group multiple ports as single Channel.		
20	Solution must support the policies to block the credit card, Bank numbers etc.… also must provide flexibility to create the polices to block file types and direction of data passing via firewall (download and upload etc..).		
21	The firewall appliance shall support minimum 10 virtual systems / virtual contexts. Virtual systems/contexts/vdom must support all the NGTP features individually.		
22	**Performance Requirements**		
23	Proposed appliance must have Threat Prevention throughput of at least 10 Gbps with Application Control, FW, IPS, Anti-malware/ Anti-Virus, Antibot & URL Filtering/web protection & DNS Security including with logging enabled in Enterprise Mix / Application Mix traffic. The performance numbers must be available on public websites or datasheet and any letter head declaration is not acceptable.		
24	Shall have Next Generation Firewall throughput of at least 20 Gbps with Application Control, FW with logging enabled in Enterprise Mix / Application Mix traffic.		
25	Must support at least 6 Million Layer 4 Concurrent Sessions or Minimum 2.5 million Layer 7 HTTP concurrent sessions/connections AND minimum 400K Layer 4 new connections/sessions per second or minimum 200K Layer 7 HTTP new connection/session per second		
26	Solution shall have minimum following ports:		
	- 8 usable 1Gig interfaces SFP/Copper		
	- 4 usable 10Gig SFP+ Interfaces		
	2 usable 40/100 gig interfaces		
	- Separate & Dedicated 1 x 1G port for out of band management		
	- Separate & dedicated port for HA connectivity		
27	Must have integrated redundant power supplies		
28	Solution architecture should have Control Plane separated physically or virtually from the Data Plane.		
29	Solution hardware should be a multicore CPU architecture with a hardened 64-bit operating system and shouldn't use any proprietary based ASIC architecture.		
30	Clause has been removed		
31	Must have minimum 240 GB of SSD storage or higher.		
32	**Network Protocols/Standards Support Requirements**		
	Solution shall support the deployment in Routed or Transparent Mode		

Sr.No.	Minimum Technical Specifications	Compliance (Yes/No)	Cross Reference
33	Must support Static, RIP, OSPF, OSPFv3 and BGP		
34	The proposed firewall shall be able to handle unknown /unidentified applications with actions like allow, block or alert		
35	The proposed firewall shall have granular application identification technology based upon deep packet inspection		
36	The proposed firewall shall warn the end user with a customizable page when the application is blocked		
37	The proposed firewall shall delineate specific instances of instant messaging/Social Network Applications (Facebook Chat, WhatsApp, Telegram, WeChat etc.)		
38	The Firewall shall provide stateful engine support for all common protocols of the TCP/IP stack.		
39	The Firewall shall provide NAT functionality, including dynamic and static NAT translations.		
40	Firewall should have creating access-rules with IPv4 & IPv6 objects wise, user/groups wise, application wise, application wise geolocation control, URL wise, zone wise, VLAN wise, etc.		
41	Should have more than 5000 pre-defined distinct application signatures (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application categories for operational efficiency		
42	Solution modules shall support authentication protocols like RADIUS/ TACACS+ etc.		
43	Proposed NGFW OEM must support zero-day attack protection with integration of on-prem Anti-APT/Sandboxing/Threat inspector appliance in future		
44	a) Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.		
45	b) Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many.		
46	c) Reverse NAT shall be supported.		
47	d) Port address translation /Masquerading shall be supported.		
48	Dynamic Host Configuration Protocol (DHCP) & Virtual Private Network (VPN) shall be supported		
49	The firewall shall support Internet Protocol Security (IPsec).		
50	support Key exchange with latest Internet Key Exchange (IKE), Public Key Infrastructure PKI (X.509)		
51	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES etc.		
52	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.		
53	IPsec NAT traversal shall be supported		
54	Solution should prevent against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection		
55	**Firewall Policy Requirements**		
56	Firewall/shall be able to configure rules based on the following parameter --		
	a) Source/Destination IP/Port/Geo locations		

Sr.No.	Minimum Technical Specifications	Compliance (Yes/No)	Cross Reference
	b) Time and date access		
	c) User/group role (After Integration with AD)		
	d) Customizable services		
	e) Combination of one or multiple of above-mentioned parameters		
57	It shall support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.		
58	Firewall shall support Access for Granular user, group & machine-based visibility and policy enforcement. It shall have following features:		
59	a) The firewall shall mask/NAT the internal network from the external world.		
60	b) Multi-layer, stateful, application -inspection-based filtering shall be supported.		
61	c) It shall provide network segmentation features with capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.		
62	d) Ingress/egress filtering capability shall be provided.		
63	e) There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.		
64	f) Basic attack protection features listed below but not limited to:		
	• It shall enable rapid detection of network attacks		
	• SYN cookie protection/SYN Flood		
	• Protection against IP spoofing		
	• Out of state TCP packets protection		
65	**Threat Prevention Feature Set**		
66	Should be capable of dynamically IPS policies/Profiles (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention		
67	Should have more than 10,000 (excluding custom signatures) IPS signatures or more		
68	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports		
69	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to security events		
70	Solution must have IOC management and provide reputation intelligence feeds. Should support the integration with custom IOC feeds		
71	The OEM must have its global threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection in form of updates/feeds		
72	Enforce policy on individual users or user groups: Policy to allow or deny certain types of traffic must be enforceable on individual users or user groups		
73	User-developed application signatures: The application control shall allow to create new application signatures & support import of snort IPS signatures		

Sr.No.	Minimum Technical Specifications	Compliance (Yes/No)	Cross Reference
74	**Product certifications**		
75	should obtain minimum EAL4+ or ICSA certification		
76	Must obtain recommended rating in NSS lab report.		
77	must obtain IPv6 ready/USGv6R1 standard certification to support IPV6 features.		
78	**Administration, Management, Logging & Reporting**		
79	The Firewall Management Solution, log server and reporting server can be either hardware appliance or VM based solution at On-prem only.		
80	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
81	All licenses shall be Enterprise class. Solution must be configured by the bidder to cater to smooth operation of the whole solution should be scalable to use more storage and compute if required.		
82	The Solution shall receive logs for the overall proposed solution in a single virtual system and shall not be separate for each module of proposed firewalls.		
83	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
84	Reporting must be integrated part of management solution and provide the industry standard compliance reports e.g., ISO27001, PCI-DSS etc.		
85	Point to be added in Management :- Solution must support multiple administrators to work in parallel without interfering to each other.		
86	Proposed firewall should have following license : Firewall , Threat prevention , URL filtering and DNS security license from day one		

7.13 Next Generation IPS

Sr.no	Minimum Requirements Description	Compliance (Yes/No)	Reference (Document/ Page No)
1	OEM/Subsidiary should have TAC & R&D facility in INDIA. OEM/Subsidiary should be present in India from last 15 Years.		
2	The Proposed solution should be a Dedicated appliance (NOT a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Appliance).		
3	Legitimate throughput handling: 20Gbps from day-1 and scalable up to 40Gbps Attack Concurrent Sessions : Unlimited Inspection Ports supported : 6 x 10G SFP+ and 6 x 1G SFP from day-1. Option for additional 8 x 1G/10G SFP+ for		

Sr.no	Minimum Requirements Description	Compliance (Yes/No)	Reference (Document/ Page No)
	future use (Break-Out should not be used to accommodate port) SSL CPS: 90,000 on RSA-2k Key The appliance should have dedicated 1 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port *Data should be publicly available		
4	System should support horizontal and vertical port scanning behavioural protection.		
5	System must be able to detect and block SYN Flood attacks		
6	The system should protect against DNS based attack		
7	System should support HTTP Challenge Response authentication without Scripts		
8	System should support In-Line, SPAN Port or equivalent method , Out-of-Path deployment modes from day 1		
9	Solution should be transparent to control protocol like MPLS and 802.1 Q tagged VLAN environment. Also, it should be transparent to L2TP, GRE, IP in IP traffic.		
10	The proposed Solution should protect against Packet Anomalies based attack such as Unrecognized L2 Format, Invalid IP Header or Total Length, Inconsistent IPv6 Headers, Invalid L4 Header Length, Invalid GRE Header etc		
11	**Tunnelling Protocols :** VLAN Tagging, L2TP, MPLS, GRE, GTP, IPinIP		
12	The proposed solution should detect and mitigate recursive domain name system attacks by analysing the monitored DNS traffic using detection function to detect an anomaly based on the baseline learnt or any other equivalent method ; and upon detection of anomaly, should perform mitigation action to filter out incoming DNS queries to a domain name under attack.		
13	Clause has been removed		
14	• Server-based vulnerabilities: — Web vulnerabilities — Mail server vulnerabilities — FTP server vulnerabilities — SQL server vulnerabilities — DNS server vulnerabilities — SIP server vulnerabilities • Worms and viruses • Trojans and backdoors • IRC bots • Spyware • Phishing • Anonymizers		
15	The proposed Device should use the following Block Actions : drop packet, Reset, Permit, Trust, Notify, Trace, Quarantine or blacklist		

Sr.no	Minimum Requirements Description	Compliance (Yes/No)	Reference (Document/ Page No)
16	The IPS should provide protection against Zero Day attacks with automatic signature within 20 seconds without human intervention. It should have anti-scanning functionality from day 1.		
17	Appliance should have anti-scanning functionality from day 1.		
18	System should have capability to allow custom signature creation along with inbuilt signature of 5000+. Custom signature should be different than inbuilt signature		
19	The proposed Solution should have Connection limit Profile to protect against session-based attacks, such as half-open SYN attacks, request attacks, and full-connection attacks.		
20	The appliance should support SSL Inspection capabilities from day 1		
21	The proposed Solution should protect against Packet Anomalies based attack such as Unrecognized L2 Format, Invalid IP Header or Total Length, Inconsistent IPv6 Headers, Invalid L4 Header Length, Invalid GRE Header etc		
22	The solution should have Signature Update, Geo-Location Blocking and Attacker based feeds from day 1		
23	Bidder should propose Separate Centralized Management & Reporting Solution from Day 1.		
24	The proposed solution should detect and mitigate attacks on all ports and protocols by analysing the monitored traffic using detection function to detect an anomaly based on different parameters configured in the solution; and upon detection of anomaly, should perform mitigation action to block the traffic or alert the admin on the same.		

7.14 SAN Switch

Sr. No	Minimum Requirement Description		Compliance (Yes / No)	Reference (Document /Page no)
1	Fibre Channel Generation	32Gbps		
2	Switch Type	Fixed		
3	Total Fibre channel port bundled with License	32 expandable to 48		
4	Fibre Channel Port Speed (Gbps)	32		
5	QSFP (FCoE)port	NA		
6	Media Type Fibre Channel	SWL		
7	Autosensing (Gbps)	16/32		
8	FCIP ports	0		
9	IP Port speed (Gbps)	NA		
10	Media Type, IP	NA		
11	FCIP performance (GbE)	NA		
12	Aggregate Switch Bandwidth FC (end to end full duplex)	1536 Gbps		
13	Aggregate Switch Bandwidth IP (end to end full duplex) (Gbps)	NA		

Sr. No	Minimum Requirement Description		Compliance (Yes / No)	Reference (Document /Page no)
14	Maximum Fabric Latency (nano second) / Locally switched port latency (nano second)	NA		
15	Blade-to Blade Latency (microsecond)	NA		
16	Maximum Frame Size	2112-byte payload		
17	Maximum IP MTU size	NA		
18	Frame Buffers	NA		
19	Class of service	Class 2		
20	Port Types	U/E/F/M/D		
21	Access Gateway Mode Support / NPIV support	NA		
22	Form factor (U)	1U		
23	AC Power Supply	Dual Redundant Hot Swappable AC Power Supply		
24	Support for DC Power Supply	No		
25	Airflow	Front-to-back airflow		
26	Non-Blocking Architecture	Yes		
27	Redundant Control Processors/Data Processor	NA		
28	Redundant active/active core switching blades	NA		
29	Redundant WWN cards	NA		
30	Total slots per chassis	NA		
31	Number of Blade Modules Required	NA		
32	Blade Module - 32 port with 16Gbps SWL SFP+ Blade Module	0		
33	Blade Module - 48 port with 16Gbps SWL SFP + Blade Module	0		
34	Blade Module - 64 port with 16Gbps QSFP+ Blade Module	0		
35	Blade Module - 48 port with 32Gbps SWL SFP+ Blade Module	0		
36	FCIP Blade Module	0		
37	FCIP Blade Connectivity Option (Gbps)	NA		
38	ISL Trunking	Yes		
39	Real time Monitoring & Threshold alerts	Yes		
40	Centralized Management Software to manage and monitor multiple Fabrics within/across multiple sites from single window	Yes		
41	ISL trunking	Yes		
42	Virtual Fabrics	Yes		

7.15 Laptop

Sr. No	Specification Parameter	Specification Value as per Corrigendum	Compliance (Yes/No)	References (Document/Page No
1	Chassis Material	Metallic		
2	Hinges	Metallic		
3	Processor Make	Intel and AMD		
4	Processor Type	Intel® Core™ i7-1355U Processor 13th Generation or higher (while quoting a higher version CPU it shall be ensured that the no. of cores/threads, processor base frequency and Cache should be equivalent or higher than the specified CPU) OR AMD 7730U Processor or higher (while quoting a higher version CPU it shall be ensured that the no. of cores/threads, processor base frequency and Cache should be equal to or higher than the specified CPU)		
5	Maximum Clock Speed	4.5 GHz or higher		
6	Memory (Offered)	16 GB or higher DDR4 3200 MHz, expandable up-to 32 GB or higher without discarding of any existing modules		
7	HDD	1TB SSD		
8	Graphics	Integrated UHD Graphics/ Integrated AMD Radeon™ Graphics or higher		
9	Bluetooth	Bluetooth 5.2 or higher		
10	WiFi	WiFi 802.11n, WiFi 802.11ac, WiFi 802.11ax		
11	Network Port	Minimum 1x 10/100/1000 Mbps		
12	I/O Ports	a) Minimum 2x USB 3.2 Gen 1 port or higher		
		b) Minimum 1x USB-C Type		
		/Thunderbolt 3 or higher		
		c) Minimum 1x HDMI 2.0 or higher		
		d) Minimum 1x Universal audio port		
13	Security Feature	a) Finger Print reader		
		b) TPM 2.0		
		c) Lock Slot (cable to be provided)		
14	Operating System (Supported)	Microsoft Windows 11 Pro or later– 64 bit, Ubuntu Latest version, Dual boot OS		
15	Operating System (Factory Pre- loaded)	Pre-loaded with only Microsoft Windows 11 Pro or later– 64 bit.		
16	Keyboard	Standard backlit keyboard		

Sr. No	Specification Parameter	Specification Value as per Corrigendum	Compliance (Yes/No)	References (Document/Page No
17	Mouse	External USB Wired Optical Mouse		
18	Battery Backup	3 Cell 50 W/hr or higher battery to provide battery backup of more than 8		
		hours		
19	Weight	Maximum 1.5 Kg		
20	Webcam	Integrated HD Webcam or higher		
21	Audio	Integrated microphone and stereo speakers		
22	Power Adaptor	USB Type-C power input/65 W External AC power adapter		
23	Accessories	Premium Backpack		
24	Warranty	Comprehensive onsite warranty of 5 years or higher.		
25	Support	a) Support should be either from OEM/Vendor participating in this quote.		
		b) Service response time should be NBD.		
		c) Downtime should not exceed 3 working days.		
		d) Vendor should either service the system or provide standby system with- in the specified time frame else warranty shall be extended by 15 days for every one day of delay		

7.16 Vulnerability Assessment

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
Policy Creation and Enforcement: The proposed solution must have the following features.			
1	Provides visibility into workload vulnerabilities using CVE and CVSS scores.		
2	Captures and analyses real-time flow and process telemetry for 6-month retention.		
3	Automatically generates and enforces per-application whitelist policies.		
Policy Management and Integration:			
4	VA scanner must be deployed as 1. Active-Active 2. Active-Passive 3. Standalone 4. Manual 5. Multi Tenancy 6. Zero Touch Deployment		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
5	VA Scanner must support automation and management: 1. Terraform 2. Ansible 3. Heat Template 4. AWS Lambda 5. Azure ARM 6. Elastic Beanstalk 7. CLI 8. SSH 9. GUI		
6	License Model for the VA scanner (On Premises). 1. Host Based 2. IP Based 3. Container Image Based 4- Container Host/POD		
Behaviour and Anomaly Detection: The proposed solution must have the following features			
7	Groups endpoints with similar behaviour into policy groups, correlates network traffic.		
8	Provides application dependency map, detailing relations and inter-dependencies.		
9	Integrates with external systems for additional context for each workload.		
10	Tracks process tree lineage and historical records over time.		
Asset Inventory			
11	The proposed VA solution must have below Asset Visibility features: 1. Provision for User to create assets inventory hierarchically like Site:- Data Centre Name, Project name, Assets Groups(IPs) 2. Continuous discovery of assets 3. Inventory visibility with elastic search like querying 4. Elastic query-based asset and vulnerability search 5. Real-time continuous inventory. 6. Updates and keep hardware inventory like CPU type, Memory size and disk partitions too 7. Should generate graphical discovery map for discovered devices and provide reports of added and removed devices on daily basis 8. Should be able to convert a query into a widget 10. Must allow saving a query so that it can be re-used		
Compliance and Management:			

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
12	Custom forensic rules creation, alerts on process behaviour deviations. The proposed VA solution must be able to conduct threat scanning of 10 IP addresses simultaneously.		
13	The size of the agent must not be more than 50MB.		
14	Types of detection included. i) Agent Support Windows (all client and server versions) ii) Agent Support Linux and Unix iii) Agent Support Mac OS iv) Agent Support AIX v) Agent Support SOLORIS		
15	The solution must provide flexible Risk scoring in Dashboard. The solution must have The ability to do low-code or no-code based response action based on a workflow. The solution must provide a comprehensive Certificate inventory and the ability to renew or revoke a certificate if required. The solution must have the ability to do low-code or no-code based response action based on a workflow		
16	VA Scanner must be based on software and hardware.		
VA scanner deployment			
17	1. Active-Active 2. Active-Passive 3. Standalone 4. Manual 5. Multi Tenancy 6. Zero Touch Deployment		
18	The VA scanner (On Premises) must support below container protection features 1. Container runtime protection 2. Gathers comprehensive topographic information about your container projects including images, image registries, and containers spun from the images etc. 3. Identify images that have specific vulnerabilities, or that have vulnerabilities above a certain severity threshold 4. Integration with various container registry like Docker registry, Quay, Harbor for scheduled or on-demand scan		
19	VA Scanner Functioning: Load balancing, Task peering, Automatic failover		
20	The solution must provide flexible Risk scoring in Dashboard. The solution must have The ability to do low-code or no-code based response action based on a workflow		
21	Number of Licences for Container Host/POD based Scanning -15		
	OEM Support Features:		
22	**1**. 24 x 7 x 365 Support by respective OEM 2. 24 x 7 x 365 Support by respective OEM from India		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
	3. OEM office in India 4. Support offices Pan India 5. Provides direct & its own payroll employee based onsite professional services for installations, configuration, validations, support etc. 6. Updating for Patches and Bug fixes within support period 7. Upgradation of version within support period		
IPv6 support and scan by hostname/IP supported:			
23	Global Threat Intelligence support: DBIR (Data Breach Investigations Report), SANS TOP20		
Asset Inventory Features			
24	1. Actionable intelligence from Threat Intel sources 2. Configuration Management Database Integration 3. To be customized based on an Asset search query & tool able to convert clicks to search query 4. Allow user to drag and drop of widgets to reposition it on dashboard 5. Widgets to be colour coded so that user can measure risk appetite 6. Highlight and risk rank criticality of assets 7. Drilldown capability from the UI (User Interface) 8. Must identify EOL(End of Life)/EOS(End of Support) for software and hardware 9. Must identify and tag every software to either Commercial and opensource software 10. Must allow daily trending within a widget 11. Flexible widgets like Pie chart, Bar chart, value based and list based		
Generic Features of Asset Inventory			
25	1. Single Management Console with RBAC (Role Based Access Control) . User site / project/ asset group to be able to handle scanning reporting quering, asset group creation and deletion independently. 2. Easy deployment 3. Scalable and extendable 4. Minimal impact on systems and networks 5. Ability to handle virtualized environments and Complete coverage for Container host, image and registry 6. Configurable colour coded widgets for visual analytics 7. Provision to engine pooling with multiple engines grouped together to run any single scan to reduce and improve scanning time by load sharing 8. Ability of Database queries to run against reporting data model, without using third-party tools, within the solution 9. Scanning engine to be able to scan IPs simultaneously and the rest of the IP's /asset scheduled for scanning (in any site) to be able to put in the scanning queue and run automatically		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
	10. While scanning is running in one or more than one sites/groups the user to be able to add new assets in the Group/sites in which scanning is running as well as in other group/sites and to be able to put the same into scanning queue 11. VA Scanner to be able to scan duplicate or overlapping IP ranges		
26	Minimum volume of IP threat can be scanned simultaneously by each scan engine:-10		
Support for major Container orchestration Platform			
27	1. RedHat OpenShift 2. OpenStack Magnum 3. Kubernetes		
Container Asset Discovery/ Inventory:			
28	1. Discover, track and continuously secure containers – from build to runtime 2. Container ready security and compliance platform 3. Complete visibility of container hosts wherever they are in your IT environment – on premises and in clouds		
29	**Threat Management:** Threat identification, impact assessment and remediation prioritization		
Container Protection Features			
30	1. Container runtime protection 2. Gathers comprehensive topographic information about your container projects including images, image registries, and containers spun from the images etc. 3. Identify images that have specific vulnerabilities, or that have vulnerabilities above a certain severity threshold 4. Integration with various container registry like Docker registry, Quay, Harbor for scheduled or on-demand scan		
31	Correlated list of features in Vulnerability Management: 1. Metasploit exploit modules available for each vulnerability 2. Malware kits available for each vulnerability		
Type of detection			
32	1.Agent-based detection (On-Premises) 2. Agentless detection 4. Agent Support Windows (all client and server versions) 5. Agent Support Linux and Unix 6. Agent Support Mac OS 7. Agent Support AIX 8. Agent support FreeBSD 9. Agent should support mobile devices		
Vulnerability Management Features			

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
33	1. Configurable monitoring and alerting features 2. Auto updating & Self managing scanners and agents 3.Ability to Track the status of vulnerability with each iterative scan 4. User login should be supported with 2 factor authentication 5. Should allow defining policy for console access with IP whitelisting 6. Tool should be able to covert running golden image of hardened OS into policy template 7. Agent and scanner should communicate directly with Management console over encryption without any other intermediate device 8. Scan result database should be encrypted 9. Tool should support plugins for CI-CD pipelines for build tools like Bamboo, Jenkin, GitLabs, etc. 10. Tool should support Cloud Workloads in Azure/VMware/OpenStack IaaS on premises 11. Tool should support Cloud Workloads in Azure/VMware/OpenStack PaaS on premises 12. Should have the ability to auto-eliminate superseding patches 13. Should have the ability to auto-eliminate vulnerabilities that can be fixed with a config change 14. Should provide information if the vulnerability has a virtual patch available 15. APIs, Scripts/Tools and zero touch deployment of scanner and agent 16. Report generation through API in cloud		
Generic Features of Vulnerability Management			
34	1. VA Scanners running on hardened OS with no root or sudo access to it 2. Ability to track ongoing progress against vulnerability management objectives 3. VA Scanner should be a physical appliance with features of self-updating and self-managed 4. VA Scanner should be tenant based virtual appliance . Means solution must have virtualisation features to create multiple tenants. 5. Agent should not work like local VA Scanner 6. Agent should be self-updating and tamper resistant 7. Agent should be able to use a proxy and do data compression 8. VA Scanner should be able to check credentials authentication before launching scan 9. Ability to fine tune agent for CPU, Memory and bandwidth 10. Scanner should have password less key communication to run agent and communicate between them, No physical password should be shared from user.		
Provision of Alerts/ Flags/Reports for			
35	1. Newly opened ports 2. Changes to ports 3. New services on ports 4. Closing of ports 5. Common vectors for attack and exploit		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
	6. Certificate health 7. Application installation / un-installation 8. Installation of new or unauthorized software 9. Upgrades or downgrades or removals of existing software		
Monitoring Features			
36	1. Provision to detect and alert new assets in the network. 2.Provision to Targeted alerts based on a security policy. 3.Certificate data insight and certificate-based vulnerabilities. 4.Provide alerts based on threat intelligence 5.Provision to monitor SSL certificates and alert on expiring SSL certificate 6. Provision to altert on installation or removal of software. 7.Whenever an asset/IP is scanned multiple time, user to be able to fetch/download each and every report of that asset/IP. 8.Each scan corresponding to that IP/asset to have unique scan ID.		
Generic Features of Monitoring			
37	1. Target alerts for each issue to the people responsible for fixing them 2. Provision of calendar-based alerts dashboard 3. Provide alert rule creation using AND / OR / ONLY-IF kind of logic. 4. Reduced risk of system changes going unnoticed 5. Provide alerts via email and CEF(Common Event Format)/Syslog 6. Provide alerting for both External and Internal IPs		
CONTEXTUAL THREAT DASHBOARD			
38	2. Displays entire threat posture at a glance 3. Group vulnerabilities that have public exploit available, can result in DoS and can propagate via lateral movement 4. Provision for search results to be further sorted, filtered and refined 5.Shareable Dashboards allow import / Export to JSON(Java Script Object Notation) format for reuse and sharing in open standard 6.Every Vulnerability should be categorized with external threat intelligence categories e.g., malware, Potential DOS, Easy to exploit, Lateral movement, High data loss 7. Inbuilt threat feeds dashboard giving view of zero days, malware and PoC of exploitable Vulnerabilities 8. Make configurable dashboard with widgets from threat and asset query results		
SECURE CONFIGURATION ASSESSMENT- Technology coverage			
39	1. Host 2. OS		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
	3. Network Device 4. Security Device 5. Storage Device 6. Database 7. Application 8. Running containers 9. Mobile OS		
Database scanning Coverage			
40	1. MS-SQL (All versions) 2. MySQL (All versions) 3. Oracle (All versions) 4. PostgreSQL (All versions) 5. DB2 6. Sybase 7. MariaDB (All versions) 8. MongoDB		
Support reporting formats			
41	1. MS Word 2. Open Office Document 3. PDF 4. CSV 5. XML 6. MS Excel		
Support CIS (Centre For Internet Security) for			
42	1. Databases 2. Network Firewalls 3. UTM Device 3. IPS (Intrusion prevention system) 4. DDOS (Distributed denial of service) 5. Routers 6. Switches 7. WAF (Web Application Firewall) 8. Load Balancer		
VA Scanner Policy			
43	1. Hardened 2. Tamper resistant		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References (Document/Page No)
44	**Accuracy of detecting Vulnerability-It should be 99.99 %**		

7.17 Server Security

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
	Server Security		
1.	The solution should have state full Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Web Reputation Device control and Recommended scan in single module or an in single agent.		
2.	The proposed solution must be able to provide Web Reputation filtering to protect against malicious web sites.		
3.	The Solution should have featured a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.		
4.	The Solution should be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.		
5.	The Solution should provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred.		
6.	The Solution should have out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services etc.		
7.	The Solution should include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits		
8.	The Solution should automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot.		
9.	The solution must protect against all kinds of viruses, Trojans and worms including but not limited to boot sector, master boot sector, memory resident, macro, stealth and polymorphism etc.; and any other forms of exploits		
10.	The solution shall provide real time integrity monitoring of critical operating system and application elements such as directories, files, registry keys and values to detect and report suspicious activity such as modifications		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
11.	On detection of a malware infection, the solution should allow removal of traces of malware from the system by cleaning up the following automatically or via remote remediation from a centralized management console : a) Detected malicious file, b) Affected registry entries, c) Any new files dropped by malware, d) Windows services created by malware, e) Any other system settings affected by malware.		
12.	The Solution should cover of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.) with fine-grained filtering (IP and MAC addresses, ports) and basic prevention of denial of service (DoS) attack		
13.	The Solution should be able to detect and protect from reconnaissance scans and solution.		
14.	The Solution should be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes.		
15.	The Solution should provide virtual protection which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs/physical servers within minutes.		
16.	The solution should support Application control, behaviour monitoring, Ransomware protection & Zero-day threat protection along with simulation engine.		
17.	The solution be on premises with Zero-day attack prevention along with customize simulation engine as per infrastructure.		
18.	The Solution should support at least Windows 10, Windows Server 2008, 2012, 2016, 2019, 2022, RHEL 32 bit and 64 bit, Solaris, Debian, Ubuntu, Oracle Linux, and SUSE.		
19.	The Proposed solution should Offers host-based firewall capabilities for network filtering.		
20.	The proposed solution must have capability to control the external devices like USB,LPT ports , Wireless devices ,external storage devices etc. It should have to control full access/read only/block mode.		
	Anti Malware features		
21.	Solution must scan, detect, clean, delete and quarantine the infected files.		
22.	Solution must clean/ delete/ block malicious codes/software in real time, including viruses, worms, Trojan horses, bot, spyware, adware, mass mailing worms and Rootkit for Windows based Operating systems /Root kit along with web shell(s) for UNIX/Linux based operating systems		
23.	Solution must have capability to scan, detect and clean the boot sector and Master boot record		
24.	Solution must have embedded behavioural analysis and protection technology apart from signature based clean/delete/quarantine for unknown threats.		
25.	Solution must scan, detect and clean or delete malicious code for protocols like POP3 /IMAP/FTP etc.,		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
26.	Solution must provide to install antivirus agent through various techniques like web based, MSI package or other methods in workgroup and Active Directory/LDAP environment.		
27.	Solution must provide to scan single file/directory/entire system and detect, clean, delete or quarantine the infected file.		
28.	Solution must provide file reputation and web reputation and blocking of intrusion using browsers like Opera, Safari, Chrome , IE etc		
29.	Solution must provide scheduled scan configuration for full-disks scan at designated time from central manager for clean, delete or quarantine infected file.		
30.	Solution must provide to prevent endpoint users from uninstalling or disabling the managed antivirus services.		
31.	Solution must provide to exclude the specified files/directories from real time and manual scan.		
32.	Solution must provide a utility program for clean uninstallation process of the corrupted antivirus.		
33.	Solution must be fully IPv4 and IPv6 compliant (dual-stackable)		
34.	Solution must provide virtualized environment		
35.	Solution must submit the suspected files for which signature has been developed		
36.	Solution must provide self-learning whitelisting, and block applications attempting to execute on any endpoint, unless explicitly allowed by administrator.		
37.	Solution must allow for creating whitelisting of application programs, DLLs and executable files and block all remaining programs, DLLs. executable files for execution.		
38.	Solution must provide prevention of tampering and hijacking of applications		
39.	Solution must have the capability to classify applications which are attempting network access and block unauthorized connections and data transfers by malicious programs.		
40.	Solution must provide to protect against zero-day attacks		
41.	Solution must have the capability to accept new software added automatically through authorized processes.		
42.	Solution must provide all the supported versions/latest versions of Microsoft Windows Operating Systems.		
43.	Solution must have the capability to generate infected systems report with their source and destination IP address.		
44.	Solution must provide to generate malware, name-wise reports based on source and destination IP address.		
45.	Solution must provide to generate user defined reports from database. In case reports are provided in raw logs, vendor must be able to generate meaningful reports by exporting into a database.		
46.	Solution must provide to generate following reports:		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
47.	Current Virus Definition.		
48.	Virus Definition updates.		
49.	Report generated must be exported to other applications like HTML, Microsoft Excel, CSV or PDF.		
50.	Graphical Charts for malwares, infected endpoints etc. for managed clients.		
51.	Solution must provide to send endpoint logs based on IP and MAC address automatically up to the central manager.		
52.	Solution must provide that the managed endpoints must send Antivirus event logs.		
53.	Solution must provide to send logs of device control and application control to the central manager		
54.	Solution must provide that the managed endpoints must send Antivirus firewall logs i.e., compliance violations and access log.		
55.	Solution must provide that the managed endpoints must send Endpoint Based Intrusion Prevention System compliance violations and access log.		
56.	Solution must provide to integrate with 3rd Party Log Analyzer Application Software like Arc-Sight.		
57.	Solution must provide a Utility program for all supported Windows operating systems for collecting logs of infected endpoints for analysing and developing signatures.		
58.	Vendor must provide log analysis of infected systems and submit required suspected files to OEM lab for new signature		

7.18 Virtual Web Application Firewall

Sr.No.	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
1	**General Requirements:**		
2	Should be a Virtual appliance with hardened OS and available for the VMware vSphere, Microsoft Hyper-V and KVM or OpenStack.		
3	Web application firewall should provide specialized application threat protection.		
4	Should protect against application layer attacks targeted at web applications.		
5	Should provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting and support OWASP application security Methodology.		
6	Should provide controls to prevent identity theft, financial fraud and corporate espionage.		
7	Solution should have provision to add application licenses as per the raised/scalable requirement.		

Sr.No.	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
8	Automatic signature updates and install		
9	Should monitor and enforce government regulations, industry best practices, and internal policies.		
10	Performance requirements		
11	Should deliver minimum 2 Gbps of throughput scalable to 3 Gbps.		
12	Interface and connectivity requirements		
13	Should support 4 no's of virtual Network interfaces		
14	**Feature specifications.**		
15	The Solution should be able to perform in multiple modes such as Active/ Passive mode, Transparent mode, proxy mode,		
16	Solution should continuously track the availability of the Servers being protected.		
17	Should have Data Leak Prevention module to analyse all outbound traffic alerting/blocking any credit card/Aadhaar No leakage and information disclosure		
18	Provide controls to meet PCI DSS compliance requirements for web application servers.		
19	Should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.		
20	Should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.		
21	Should support automatic signature updates to protect against known and potential application security threats.		
22	Ability to define different policies for different applications		
23	Ability to create custom attack signatures or events		
24	Ability to combine detection and prevention		
25	Should protect certain hidden form fields.		
26	Must provide ability to allow or deny a specific URL access/IP(s).		
27	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, converting back slash to forward slash character etc..		
28	Must support Website anti defacement.		
29	A given user must be enforced to follow a sequence of pages while accessing.		
30	The WAF should support IP Reputation Service and able to provide up to date information about threatening sources.		
31	Support IPv6 for Reverse Proxy deployments and It should also Support IPv4 to IPv6 and IPv6 to IPv4 communication		

Sr.No.	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
32	Device should be able to control BOT traffic and It should be able to block known bad bots and fake search engine requests		
33	WAF should support File Upload Violation & should provide support for scanning of malicious content		
34	The Solution should protect against HTTP parameter pollution attacks.		
35	The solution should be able to employ connection pooling technology to optimize backend network operations and server resources		
36	It shall have features to hide errors from server and redirect to customized page		
37	It should allow IP addresses or IP address range for bypassing applied security policy for one particular hosted application but should not bypass others.		
38	Web Application firewall should facilitate in hiding/masking sensitive parameters in all user logs.		
39	Actions taken by WAF to prevent malicious activity should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address permanently or for a time period .		
40	Should inspect Simple Object Access Protocol (SOAP) and extensible Mark-up Language (XML), in addition to HTTP (HTTP headers, form fields, and the HTTP body).		
41	The negative security model should detect and protect attack based on Signature (Regular expression) and complex logic (logical AND, Logical OR) against incoming URL request and the same may be extended for all parts (i.e., URI, parameters, headers, cookies.)		
42	The positive security model should validate URLs, directories, cookies, headers, form/query parameters, HTTP methods, File upload Extensions, Allowed meta characters etc		
43	The WAF should support profiling to configure fine grained controls for each deployed web application		
44	The solution should support all operating systems/Development frameworks and their versions including but not limited to Windows, AIX, Unix, Linux, Solaris, HP Unix.		
45	The Solution should provide HTML rewriting functionality (e.g., edit, add, delete request and response header, rewrite and redirect the URL in the request, rewrite response body etc).		
46	Clause has been removed		
47	The Solution should have the ability to generate and issue CAPTCHA or equivalent queries to challenge suspicious clients.		

Sr.No.	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
48	Auto Learn		
49	Should have the capability to Auto-Learn Security Profiles required to protect the Infrastructure.		
50	Should provide a statistical view on collected application traffic		
51	auto-learn options should be available to tweak and fine tune rules		
52	WAF may continue to provide protection even while in learning mode.		
53	Brute Force Attack		
54	Should have controls against Brute force attacks		
55	should Detect brute force attack (repeated requests for the same resource) against any part of the applications		
56	Custom brute force attack detection for applications that do not return 401.		
57	The solution should provide protection from application layer DDoS attacks such as slowloris, RUDY and slow read attacks		
58	Protection against SYN-flood type of attacks		
59	Cookie Protection		
60	Should be able to protect Cookie Poisoning and Cookie Tampering.		
61	Strict Protocol Validation		
62	Must support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP1.1		
63	Should support restricting/Controlling the methods used.		
64	Should validate header length, content length, Body length, Parameter length, body line length etc..		
65	SSL		
66	It shall support hosting/terminating of SSL web applications and should allow to upload the certificates and private/public key pairs for the Web servers.		
67	In termination mode, the backend traffic (i.e., the traffic from the WAF to the web server) can be encrypted via SSL		
68	Are all major cipher suites should be supported by the stable upgraded SSL/TLS implementation.		
69	should provide protection against SSL Based attacks.		
70	Should support for SSL off loading		
71	High Availability and load balancing		
72	Should support High Availability in active/passive & active/active mode		
73	WAF appliance should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers.		
74	Vulnerability Scanning.		

Sr.No.	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
75	Shall be integrated with Third Party Vulnerability scanning tools to provide virtual patching with required understanding of WAF policy		
76	Authentication and Administrative access.		
77	Should support Secure Administrative Access using HTTPS and SSH		
78	Should support Role Based Access Control for Management		
79	Ability to remotely manage boxes		
80	Management User Interface support for both GUI and CLI access.		
81	Separate network interface for SSH/HTTPS access.		
82	Support for trusted hosts		
83	Role-based management with user authentication.		
84	Centralized Management / Reporting of multiple WAF devices for large distributed environment.		
85	Should support two Factor Authentication for login into the Management Web GUI		
86	Logging, Reporting and Troubleshooting**.**		
87	Ability to identify and notify system faults and loss of performance		
88	Should support Log Aggregation		
89	Should support multiple log formats such as CSV, Syslog, TXT, etc..		
90	Should support inbuilt Reporting and sending the report via E-Mail		
91	Should support report formats in PDF,HTML/WORD/RTF, etc..		
92	Reports should be customizable.		
93	Report Distribution Automatically via email		
94	Should generate comprehensive event reports		
95	Should be able to monitor real-time HTTP throughput		
96	ALL Logs must have compliance to separate Log Server/SIEM solutions as per standard norms.		
97	Alerts to be raised to SOC team through Email, Syslog, SNMP Trap, Notification etc for blocking the traced malicious IP source causing specific attack		
98	Shall support to generate reports like pie-chart, bar-chart based on user defined security compliance baseline.		
99	Shall allow commands from WAF for Troubleshooting network related issues like Ping, traceroute.		
100	It shall support to generate vulnerability reports based on standard vulnerability database like CVE, NVD etc.		
101	**Backup Solution**		

Sr.No.	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
102	It shall support to take full secure configuration back up on a physical disk/VM disk or SAN/NAS storage.		
103	**Service Support**		
104	OEM should be able to deploy the Web application firewall and remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.		
105	System should have Open Stack Neutron plugins or API integration should be supported.		

7.19 Authentication, Authorization and Accounting (AAA)

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
1	The solution must support authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+		
2	The solution should provide authentication, user or administrator access and policy control for centralized access control. The solution must support an integrated user repository in addition to integration with existing external identity repositories such as Microsoft Active Directory servers, LDAP servers.		
3	Authentication protocols: The solution must support authentication protocols like PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication through Secure Tunnelling (FAST), EAP-Transport Layer Security (TLS), and PEAP-TLS.		
4	The solution must support a rules-based, attribute-guided policy model that provides access control policies, which can include authentication protocol requirements, device restrictions, time-of- day restrictions, and other access requirements.		
5	The solution must support a web-based GUI centralised management for primary and secondary instances.		
6	The centralised management must support management of software upgrades on both primary and secondary instances.		
7	The solution must support AAA features for TACACS+-based device administration on both IPv4 and IPv6 networks.		
8	The solution must support high availability from day one.		
9	The solution must support a programmatic interface for create, read, update, and delete operations on users and identity groups, network devices, and hosts (endpoints) within the internal database.		
10	The solution must include monitoring, reporting, and troubleshooting component that is accessible through the web-based GUI.		
11	The solution must support central database for all user accounts and centralized control of all user privileges, which can distribute throughout the network-to-network switches and access points		
12	The solution must be able to provide AAA services for wired and wireless LAN, firewalls, and VPN.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
13	Shall be able to provide for diverse type of network devices like switches, routers, firewalls, VPN using AAA		
14	Shall be able to provide IEEE 802.1x authentication services for network switches and wireless access points		
15	Shall support Lightweight Directory Access Protocol (LDAP) authentication forwarding for user profiles stored in directories from leading directory vendors		
16	Shall provide features to define different access levels for each administrator and the ability to group network devices to enforce and change of security policy .		
17	Shall provide access control lists based on time-of-day, and day-of-week access restrictions		
18	Shall provide for defining sets of ACLs that can be applied per user or per group for layer 3 network devices like routers, firewalls and VPNs		
19	Shall provide for certificate revocation using the X.509 CRL profile for enhanced security with EAP-TLS		
20	The solution must be software based and shall be deployable on a Virtual Machine.		

7.20 NAC Solution

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
1	The NAC solution must eliminate 'blind spots', and provides a wealth of actionable data.		
2	Solution should be best in class fully out-of-band model, deployed and managed centrally with flexible integration options for wired, wireless and VPN infrastructure. It can also use SPAN port or SNMP dependent integration.		
3	Proposed NAC solution must have native integration with proposed AAA,AD,SSO and Access Control solution for user authentication which should enforce second factor of authentication as well to ensure zero trust network access control.		
4	Solution should support discovery, control of all end point and should be able to ingest IOC natively / threat feed from proposed NGFW/Anti-Spam/Anti-APT solutions.		
5	Solution must support perpetual/subscription licensing model. The solution should be sized for minimum of 50,000 concurrent devices/users. In case of subscription based licencing, the validity should be of 66 months		
6	The NAC solution must offer Network Visibility, Device Profiling, Easy and powerful Onboarding process, Endpoint Compliance, Network Provisioning and Threat Identification module provide security actions through integration.		
7	NAC solution can be deployed in virtual machines VMWare, Hyper-V, AWS, Azure, KVM etc.		
8	The system should not be based on SPAN port integration.		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
9	Allows organization to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent security policy.		
10	Must authorize access via VLAN assignment and/or applying access control lists (ACLs).		
11	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).		
12	The proposed solution must be capable of working with endpoint agents and agentless.		
13	NAC solution must be integrated with infrastructure devices by using, CLI, Syslog, API and RADIUS.		
14	NAC solution must be vendor agonistic solution suited for heterogeneous network.		
15	NAC solution must be integrated with existing network and security equipment and application.		
16	The proposed solution must be capable of working with endpoint agents and agentless.		
17	NAC solution must have the ability to inventory all devices on a network including non-PC equipment like printers, smart phones, IP-phones, and appliances.		
18	Must authorize access via VLAN assignment and/or applying access control lists (ACLs).		
19	Clause has been removed		
21	Proposed solution should support integration with proposed firewall via API, Scripts, IP etc for pre-assessment and profiling of device and users and should be able to provide access control on basis of the intelligence gathered .		
22	The NAC solution MUST be best in class fully out-of-band NAC solution that fits in any heterogeneous network.		
23	Guest management capabilities must be quickly and easily to set up guest account without engaging IT staff.		
	Endpoint profiling Requirements		
24	NAC solution must have the ability to get inventory all devices on a network and profiling for non-PC equipment like printers, smart phones, IP-phones, and appliances.		
25	Must support profiling for Client and clientless devices based on a DHCP fingerprint, NetFlow, Vendor OUI, location, IP range, HTTP/HTTPS, Network traffic, TCP & UDP, SSH & Telnet, and the existence of the persistent agent		
26	Must support profiling for IP surveillance cameras based on ONVIF/ MAC ID/ Vendor ID with different device profiles.		
27	Must support Profiling for windows based on WinRM and WMI/ DHCP/ AD profile		
28	Must support Script based Device Profiling method to execute the command line scripts to profile the device.		
29	The system must collect detailed asset information about MAC address, Logged on user, OS, NIC vendor, Switch Port, etc.,		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
30	Must provide the ability to create custom profiling rules with more than one profiling methods in single rule to profile the device. And it must have an option to verify the rule every time when the device connects to the network to avoid MAC spoofing.		
	Authentication and Enforcement Requirements:		
31	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.		
32	Must support flexible authentication options to include, 802.1X, Web Authentication and MAC Authentication		
33	Must support RADIUS MAC-address whitelisting & blacklisting natively		
34	Must support Built-in local RADIUS server with Multiple Winbind instances which can process RADIUS MAC and 802.1x EAP authentication and proxies 802.1x EAP authentication to an external RADIUS server like Microsoft IAS and Free RADIUS		
35	Must support RADIUS logging and information on the dashboard to see pass/fails of 802.1x/MAB authentication and logs of failed authentications can be exported.		
36	LDAP — Microsoft Active Directory, OpenLDAP, Google SSO, Kerberos		
37	Should be able to append additional attributes to incorporate the authenticator's location, device type, vendor etc apart from the user attributes.		
38	Proposed solution must integrate with common vulnerability assessment vendors list: Qualys, Tenable		
	Endpoint Compliance and Remediation Requirements		
39	The solution must support both agent-based (Persistent Agent, Dissolvable Agent) and agentless endpoint inspection.		
40	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.		
41	IT should have an option to create custom scan for monitoring all the service and process scan with schedule time.		
42	The solution must provide a quarantine role that ties into the integrated patch management systems. Within this quarantine role the solution shall provide a "self-remediation" web captive portal. Non-compliant devices must be quarantined dynamically and provided with instructions for self-remediation or can be interfaced with auto-remediation systems such as BigFix and PatchLink.		
43	Proposed solution must be able to Disable Internet connection sharing, Detect Network bridges.		
44	Should support Detection of wireless connectivity to Dual-homed connections.		
45	Guest Management		

S. No.	Minimum Requirements Description	Compliance (Yes/No)	References(Document/Page No)
46	Guest Management should support notification by SMS and email. It should support Mail to SMS, API, HTTPS-based SMS gateway integration.		
47	Must support Customization of SMS and E-Mail messages for Self-Registered and Pre-Registered Guests		
48	Guest Management should be configurable to meet various requirements such as short or long-term guests, conference mode or self-registered guest		
49	Solution should support limited and controlled administrative access for Guest Management Only.		
50	Clause has been removed		
51	Guest Management should support employee sponsorship workflow.		
52	Must support API integration with the various Social Media sites Facebook, Google, LinkedIn, Outlook, Twitter and Yahoo.		
	Post Connect Assessment		
53	The proposed solution MUST provide native integration with proposed SOAR Technology.		
54	The proposed NAC must have bidirectional integration with proposed AAA solution for user authentication which must enforce 2nd factor of authentication before allowing network access to ensure zero trust principal.		

Note: The MSP need to provide the compliance to technical specification of each of the services as per the format mentioned in this section on its letter head. Deviation (if any) shall be the sole discretion of Supreme Court of India/ NICSI. Compliance sheet to be counter signed by authorized signatory of MSP.

8. Annexure: Un-priced BOQ

Sr. No	Item Description	Qty
	Hardware Items	
1	Compute servers(2 Proc. Server-32 Core each.)	24
2	Object Storage (500 TB)	1
3	Unified Storage (500 TB)	1
4	Archival Storage (1 PB)	1
5	Backup Solution (500 TB)	1
6	Spine Switch	2
7	Leaf Switch	22
8	OOB Switch / OOB Aggregator Switch	10
9	SDN/Fabric Controller	3
10	Router	2
11	Network operations appliance	3
12	Next Generation Firewall	2
13	Next Generation IPS	2
14	SAN Switches	2
15	Laptops	10
	Software Items	
16	Vulnerability Assessment tool	150 VMs
17	Server Security	150 VMs
18	Virtual Web Application Firewall (2 Gbps)	5 licenses
19	Network Access Control solution	1000
20	Authentication, Authorization and Accounting (AAA)	100 Devices
21	Redhat Openstack Premium for 5 years (2 socket*)+ LDAP	24 Servers

Note:

1. [+] In the case of socket-based licensing, 16 cores shall be treated as one socket.
2. The offered switches such as Network and SAN switches shall support both side airflow management and the bidder after receiving the contract shall confirm with Supreme Court of India/ NICSI exact number of switches with port side exhaust and portside intake airflow. Cold-aisle containment is used in this data centre for airflow management. In the Server Racks, the SAN/Network Switches shall be proposed with port-side exhaust whereas in the Aggregation & Core Racks the switches shall be with port-side intake.
3. All the warranty, support and licenses shall be effective from the date of the acceptance of the overall solution as per the scope of work.

9. Annexure: Warranty

Sl. No	Minimum Requirement	Compliance
1	The complete systems should be under 5 (Five) years on-site comprehensive warranty support service from the date of acceptance of the solution as per the scope of work	
2	During warranty period besides service/maintenance of Hardware and System Software, all software upgradation, bugs/ patches and services shall be provided free of cost by the vendor.	
3	**The Bidder should fulfill the following conditions during warranty period:**	
3(a)	Bidder will maintain enough spares in India, so as to provide satisfactory on-site comprehensive maintenance services during the warranty period. Bidder will indicate the level of spares, which will be stored by them in India for providing comprehensive on-site warranty services. Bidder will also provide a status report every six months through e-mail to Supreme Court of India about the support related complaints lodged by different users and availability of spares at the Bidder warehouse.	
3(b)	Bidder would provide the helpdesk support services through telephone/e-mail where users can lodge their complaint.	
3(c)	Any system failing at subsystem level at least three times in three months, displaying chronic system design or manufacturing defects or quality control problem or downtime penalty become more than 15% in a year, shall be totally replaced by the vendor at his cost and risk within 30 days. Failing which appropriate action including forfeiture of PBG may be initiated against Bidder after a notice period of a week.	
3(d)	Bidder shall visit each site at least once in every six months to carryout preventive maintenance and fine-tune the performance of the supplied systems besides regular service calls during warranty period.	
3(e)	On completion of the Warranty period, the PBG without any interest accrued shall be released after submission of satisfactory warranty support certificate from support coordinator to Supreme Court of India. If considered necessary, suitable amount of penalty shall be recovered from the Vendor out of either due payments or from their PBG while releasing the PBG.	

10. Annexure: Format for Price Breakup (GTV)

Sr No.	Component	Amount (including Tax/ GST)
1	Table 1 - Cost of ICT Infrastructure Components	Total Cost C1 as per Table 1
2	Table 2 – Cost of Software items (subscription & support cost*)	Total Cost C2 as per Table 2
3	Table 3: Cost of Operation and Maintenance	Total Cost C3 as per Table 3
Grand Total Value		**Total Cost C1 + C2+ C3**

Grand Total Value (GTV) = Total Cost C1 + Total Cost C2 + Total Cost C3

Grand Total Value (GTV) (in words) = _____

(All values are inclusive of taxes/GST)

10.1 Table 1 – Cost of ICT Infrastructure Components

Sl.No	Item Description	Hardware with one year warranty Cost	Yearly Support / AMC cost from 2nd year onwards	Total Hardware Cost with 5-year Support/ AMC	Quantity	Total cost	Rate of GST/Taxes	Total cost Inclusive of GST/Taxes
		A	B	C=A+(4*B)	D	E=C*D	E	
1	Compute Servers (2 Proc. 32 core each)				24			
2	Object Storage (500 TB)				1			
3	Unified Storage (500 TB)				1			
4	Archival Storage (1 PB)				1			
5	Back Up Solution (500 TB)				1			
6	Spine Switch				2			
7	Leaf Switch				22			
8	OOB Switch / OOB Aggregator Switch				10			
9	SDN/ Fabric Controller				3			
10	External Router				2			
11	Network Operations Appliance				3			
12	Next Generation Firewall				2			
14	Next Generation IPS				2			
15	SAN Switch				2			
16	Laptops				10			
Total Cost C1								

Note:

The quoted rate must be inclusive of supply, installation, integration and 5-year onsite warranty support with upgrades, updates and patches.

10.2 Table 2 – Cost of Software items (Subscription & support cost*)

Sl.no	Item Description	UOM	Yearly Cost Exclusive of GST/Taxes				Rate of GST/Taxes	Total Cost (inclusive of GST/Taxes)
			QTY	Yearly Unit Charge	5 Year unit Charge	Total Cost		
			A	B	C = B x 5	D = A x C		
1	Vulnerability Assessment tool	VM	150					
2	Server Security	VM	150					
3	Web Application Firewall (2 Gbps)	License	5					
4	Network Access Control Solution	Users	1000					
5	Authentication, Authorization and Accounting (AAA)	No. of devices	100					
6	Redhat Openstack Premium for 5 year (2 socket) + LDAP	Server	24					
	Total Cost C2							

Note:

The subscription and support charges will be paid annually at the beginning of each year.

10.3 Table 3 – Cost of Operation and Maintenance

Table 3 – Cost of O&M services									
Sl.no	**Item Description**	**Yearly O&M Cost (Exclusive of GST/Taxes)**						**Rate of GST/Taxes**	**Total Cost (inclusive of GST/Taxes)**
		Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Total Cost for 5 years**		
1	Operation and Maintenance								
	Total Cost C3								

Note:

1. Operation and Maintenance charges will be paid quarterly by on pro-rata basis after providing the O&M support.
2. Supreme Court of India/NICSI may extend the contract for additional two years (6th and 7th year) based on the rates discovered for the 5th year on mutual understanding with the MSP.

Important Note:

1. Prices in Financial Bid should be quoted in the above format. All prices should be quoted in Indian Rupees and indicated both in figures and words. In the event of mismatch, prices in words will prevail. The GTV shall be computed as per the Total Cost of each of the below annexed tables, i.e., Table 1, Table 2 and Table 3.
2. With reference to **the Annexure VII: Un-Priced BOQ**, in case the functionalities of more than one line item are complied with a single line item being proposed by the MSP, then the rate needs to be quoted only at one place with zero price quoted at all other related line items in the **Annexure IX: Format for Price Breakup (GTV)**, with relevant remarks against each such zero value line items.