RailTel Corporation of India Ltd

(A Mini Ratna PSU under Ministry of Railways)

NOTICE INVITING EXPRESSION OF INTEREST (EOI)

EOI No.: RailTel/SR/SBC/NSIL(IT-INFRA) /01 Dated 10-07-2025

For finalising BA/SI to participate in the tender called for by NSIL Tender No: NSIL/RFP/IT/UPG/2025/01 Dt: 12/11/2024 for "Supply, Installation, Commissioning, Operation and Maintenance of Upgradation of IT Infrastructure"

RAILTEL CORPORATION OF INDIA LIMITED
No-6/1, 12th Main,
Opp-Mount Carmel College,
Vasanthnagar, Bangalore 560 052
https://www.railtelindia.com

रेलटेल कॉर्पोरेशन ऑफ इंडिया लिमिटेड
(रेल मंत्रालय के अधीन एक मिनी रत्न सार्वजनिक उपक्रम)
नंबर-6/1, 12वीं मुख्य, माउंट कार्मेल कॉलेज के सामने,
वसंतनगर, बैंगलोर 560052

निविदा आमंत्रण सूचना

ईओआई नोटिस संख्या: रेलटेल/एसआर/एसबीसी/एनएसआईएल(आईटी-इन्फ्रा) /01 दिनांक 10-07-2025

रेलटेल कॉर्पोरेशन ऑफ इंडिया लिमिटेड, (इसके बाद "रेलटेल" के रूप में संदर्भित) केवल एनएसआईएल, बैंगलोर के लिए उपयुक्त भागीदार के चयन के लिए रेलटेल के सूचीबद्ध बिजनेस एसोसिएट्स (बीए) बिजनेस पार्टनर (बीपी) / आईटी-आईसीटी बिजनेस पार्टनर्स से निविदा संख्या: *एनएसआईएल/आरएफपी/आईटी/यूपीजी/2025/01 दिनांक: 12/11/2024 के लिए* के साथ संलग्न विवरण और विनिर्देशों के अनुसार "*"आईटी अवसंरचना के उन्नयन की आपूर्ति, स्थापना, कमीशनिंग, संचालन और रखरखाव* अनुबंध" के लिए ईओआई आमंत्रित करता है।

ईओआई अनुसूची और अन्य विवरण इस प्रकार हैं:

1	वेबसाइट के माध्यम से ईओआई की उपलब्धता	10-07-2025 को 13:00 बजे से
2	बोली जमा करने की आरंभ तिथि	10-07-2025 को 13:00 बजे से
3	ऑफर जमा करने की अंतिम तिथि	15-07-2025 को 17:00 बजे से पहले
4	बोलीदाताओं के प्रस्तावों को खोलना	15-07-2025 को 17:30 बजे
5	ईओआई की अनुमानित राशि	Rs.30,00,00,000/-
6	टोकन बयाना राशि जमा	₹ 5,00,000/-**
7	निष्पादन बैंक गारंटी	एलओए का 5%
8	जेवी/कंसोर्टियम की अनुमति	नहीं
ऑफर https://railtel.enivida.com पर प्रस्तुत किए जाएंगे ।		

**सफल बोलीदाता को रेलटेल की बोली अंतिम ग्राहक को प्रस्तुत करने से पहले ₹ 70,00,000/- की शेष बयाना राशि जमा करनी होगी।

एनएसआईएल, बैंगलोर के सभी नियमों और शर्तों में काम का दायरा, आईटीटी, जीटीसी, भुगतान, एसएलए और जुर्माना, वारंटी आदि शामिल हैं, सभी बोली लगाने वालों द्वारा अनुपालन किया जाएगा और सफल भागीदार के साथ बैक टू बैक आधार पर लागू होगा। इस कार्यालय से एलओआई/एलओए/पीओ/एसओ जारी होने की तारीख से 03 महीने के भीतर सभी प्रकार से पूरा कार्य पूरा किया जाएगा।

एनएसआईएल, बैंगलोर का निविदा दस्तावेज इस ईओआई के अंत में रखा गया है। उद्धृत मूल्य सभी करों, शुल्कों, लेवी आदि सहित होगा।
सभी दस्तावेजों को पृष्ठ संख्या के साथ उचित अनुक्रमण और हस्ताक्षर के साथ प्रस्तुत किया जाना चाहिए।
किसी भी स्पष्टीकरण के लिए निम्नलिखित नामित अधिकारियों से संपर्क किया जा सकता है:

किसी भी स्पष्टीकरण के लिए निम्नलिखित नामित अधिकारियों से संपर्क किया जा सकता है:

प्रथम स्तर
आलोक रंजन
सहायक महाप्रबंधक/विपणन-तकनीकी
ईमेल: alok@railtelindia.com

दूसरा स्तर
कुमार कल्याण सुन्दरम
महाप्रबंधक/बैंगलोर
ईमेल: kumar@railtelindia.com

बोलीदाताओं से अनुरोध है कि वे ई निविदा पोर्टल पोर्टल के साथ पंजीकृत हों और किसी भी संशोधन/शुद्धिपत्र के लिए समय-समय पर जांच करें।

RAILTEL CORPORATION OF INDIA LIMITED

(A Mini Ratna PSU under Ministry of Railways)
No-6/1, 12th Main, Opp-Mount Carmel College,
Vasanthnagar, Bangalore 560052

Notice Inviting Tender

EOI Notice No: RailTel/SR/SBC/NSIL(IT-INFRA) /01 Dated 10-07-2025

RailTel Corporation of India Ltd., (hereinafter after referred to as "RailTel") invites EOIs from RailTel's Empanelled Business Associates (BA) Business Partner (BP)/ IT-ICT Business Partners only for the selection of suitable partner for NSIL, Bangalore Tender No: **NSIL/RFP/IT/UPG/2025/01 Dt: 20/06/2025** for " **SUPPLY, INSTALLATION, COMMISSIONING, OPERATION AND MAINTENANCE OF UPGRADATION OF IT INFRASTRUCTURE"** as per the description and specifications enclosed herewith.

The EOI schedule and other details are as under:

1	Availability of EOI through Website	From 13:00 Hrs. of 10-07-2025
2	Bid Submission Start Date	From 13:00 Hrs. of 10-07-2025
3	Last date for submission of offers	15-07-2025 before 17:00 Hrs
4	Opening of Bidder's offers	17:30 Hrs of 15-07-2025
5	Estimated Amount of EOI	Rs.30,00,00,000/-
6	Token Earnest Money deposit	Rs.5,00,000/-**
7	Performance Bank Guarantee	5% of the LoA %
8	JV / Consortium	Not allowed
Offers shall be submitted in https://railtel.enivida.com		

** **The successful bidder shall submit balance Earnest Money deposit of Rs.70,00,000/- before submission of RailTel's Bid end customer.**

All the terms & conditions of NSIL, Bangalore including Scope of work, ITT, GTC, Payments, SLA & Penalties, warranty etc., shall be complied with by all bidders and applicable on back-back basis with the successful partner. Entire work shall be completed in all respects within 03 months from the date of issue of LoI/LoA/PO/SO from this office.

The tender document of NSIL, Bangalore is placed at the end of this EoI. Price quoted shall be all inclusive of taxes, duties, levies etc.,

All the documents must be submitted with proper indexing with page numbers & signed.

For any clarification following designated officials may be contacted:

1st Level
Alok Ranjan
AGM/Mktg
Email: alok@railtelindia.com
Contact Number:9717644178

2nd Level
Kumar Kalyana Sundaram
General Manager/TM/Bangalore
Email: kumar@railtelindia.com
Contact Number: 9717644416

The bidders are requested to get registered with eNivida portal and do check from time to time for any Amendments/Corrigendum. For any interpretation, English version of NIT will be final.

Table of Contents

Annexure details:

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.

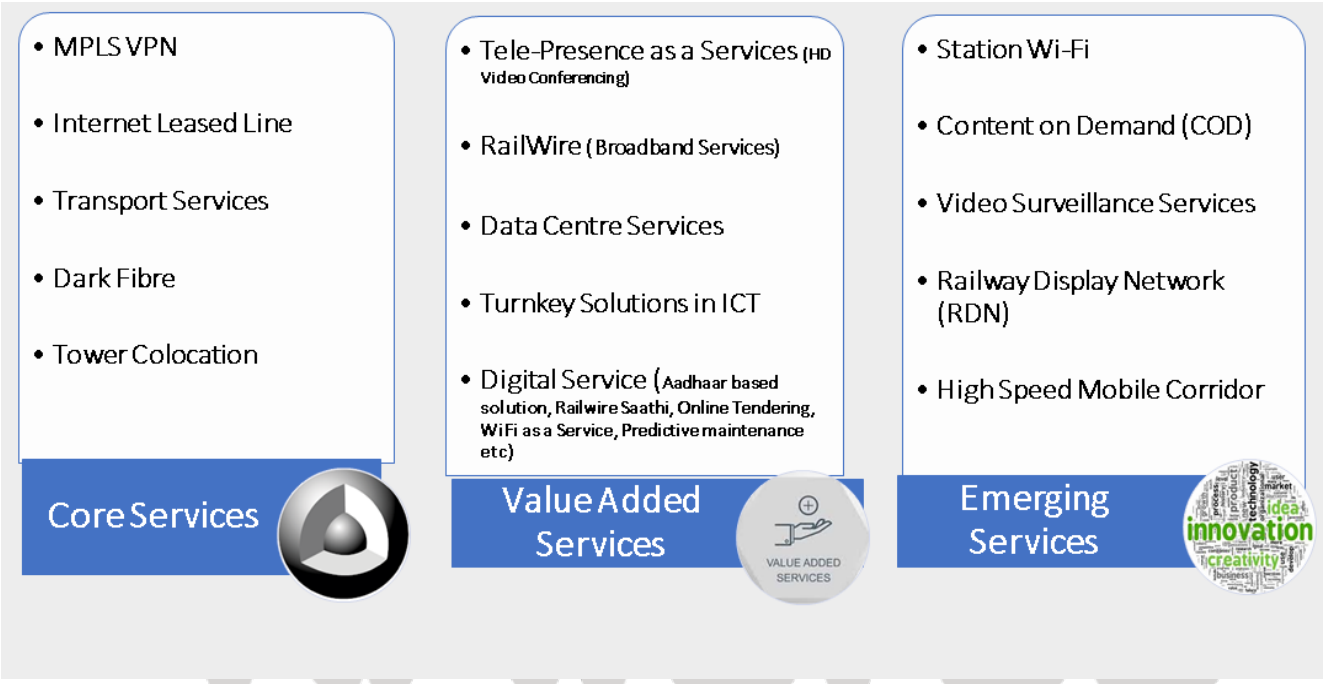
RailTel has approximately 60000 Kms of OFC along the protected Railway tracks. The transport network is built on high capacity DWDM and an IP/ MPLS network over it to support mission critical communication requirements of Indian Railways and other customers. RailTel has Tier-III Data Center in Gurgaon 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):

a) Licenses & Service portfolio:

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



b) CARRIER SERVICES

1. 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
2. Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
3. Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks
4. Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

c) ENTERPRISE SERVICES

1. Managed Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
2. MPLS VPN: Layer-2 & Layer-3 VPN available for granularities from 2 Mbps & above
3. Dedicated Internet Bandwidth: Experience the "Always ON" internet connectivity at your fingertips in granularities 2mbps to 155mbps

d) RETAIL SERVICES

Rail wire: Triple Play Broadband Services for the Masses. It is a pilot project undertaken by RailTel and currently services are offered out of Bangalore and nearby places.

2. Project Background and Objective of EOI

RailTel intends to participate in the **NSIL** Tender No: NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025for "SUPPLY, INSTALLATION, COMMISSIONING, OPERATION AND MAINTENANCE OF UPGRADATION OF IT INFRASTRUCTURE" as per the description and specifications enclosed herewith.

Accordingly, RailTel invites EOIs from RailTel's Empaneled Business Associates (BA) Business Partner (BP)/ IT-ICT Business Partners for the selection suitable partner for bidding in NSIL, BANGALORE Tender No: NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025for "SUPPLY, INSTALLATION, COMMISSIONING, OPERATION AND MAINTENANCE OF UPGRADATION OF IT INFRASTRUCTURE" as per the description and specifications enclosed herewith.

3. Scope of Work

The scope of work is as mentioned in the NSIL, BANGALORE Tender No: for NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 for " SUPPLY, INSTALLATION, COMMISSIONING, OPERATION AND MAINTENANCE OF UPGRADATION OF IT INFRASTRUCTURE" as per the description and specifications enclosed herewith.

3.1 **Schedule of Requirement** For detailed scope of work, may please refer to NSIL, BANGALORE tender document attached as part of EoI. RailTel intend to select a partner who is willing to accept all terms & conditions on back-to-back basis for their scope and portion of work. *In case of any discrepancy or ambiguity in any clause/ specification pertaining to scope of work area, the Tender released by end Customer (i.e. NSIL, BANGALORE) shall supersede and will be considered sacrosanct. (All associated clarifications, responses to queries, revisions, addendum, and corrigendum, associated Prime Service Agreement (PSA)/ MSA/ SLA also included).*

4. Response to EOI guidelines

4.1 Language of Proposals

The proposal and all correspondence and documents shall be written in English.

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 **Partner** 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 in ink by the bidder including the closing page in token of his having studies the EOI document and should be submitted along with the bid. A copy of signed EOI along with it's all Corrigendum/Addendum is required to be submitted through RailTel portal duly signed digitally.

4.4 Period of Validity of bids and Bid Currency:
Bids shall remain valid for a period of Six Months(180 days) from the date of opening of Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 of NSIL, BANGALORE. If any extension is required by customer, then the same will be extended for further period.

4.5 Negotiation:

RailTel reserves the right to negotiate with the bidder to make the bid competitive. The tenderer/s shall not increase his/their quoted rates including payment terms in case the RailTel Administration negotiates for reduction of rates. Such negotiations shall not amount to cancellation or withdrawals of the original offer and the rates originally quoted will be binding on the tenderer/s.

4.6 All offers in the prescribed forms should be submitted before the time and at fixed for the receipt of the offers. In case the schedule of requirement quoted by tenderer is incomplete with reference to tender document, the offer is liable to be rejected.

4.7 ATTESTATION OF ALTERATION:

No scribbling is permissible in the tender documents. Tender containing erasures and alterations in the tender documents are liable to be rejected. Any corrections made by the tenderer/ tenderers in his /their entries must be signed and stamp (Not initiated) by him/them.

4.8 The offer should be submitted at https://railtel.enivida.com as mentioned in the NIT. The offer should be complete in all aspects.

4.9 The bidder should submit along with all the applicable documents as per the EOI

4.10 Information to Bidder

4.10.1 Guidelines for preparations of response to this EoI - Bidder are requested to follow the below guidelines while preparing the response to EoI.

a. The price bid should be in format provided in the Annexure-I, any bid not found responsive to the details mentioned in this document may be rejected.
b. The bidder is requested to review the response before submission as the submitted responses shall be considered final and revisions may not be permitted unless there are genuine reasons for such revisions.
c. Bidder should download the document and sign each page & fill the bid sheet (Annexure-I) attach all documents as required for this EOI document and submit the complete bid as explained in the EOI document. Late and delayed response to this EOI shall not be considered.

4.10.2 Bid Earnest Money (EMD): Rs.5,00,000/- to be paid in the form of RTGS/NEFT/DD along with the offer as a token EOI EMD and the successful bidder shall submit balance EMD of Rs.70,00,000/- before submission of RailTel's bid to end customer in the form of RTGS/NEFT/DD/irrevocable Bank Guarantee in favour of RailTel Corporation of India Ltd as detailed below:

Bank Detail for RTGS:	**Company Tax Details**
Name: RailTel Corporation of India Ltd Bank: Union Bank of India Branch: RP Road, Secunderabad A/C Number : 327301010373007 IFSC Code : UBIN0805050 MICR Code: 500026009	PAN : AABCR7176C GSTN: 29AABCR7176C1Z9

4.10.3 Security Deposit / Performance Bank Guarantee: The selected Partner shall have to submit a Bank Guarantee against Security Deposit in proportion to the ordered value to RailTel as back-to-back arrangements for the Bid. The rate and value of SD/PBG shall be as per Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 of NSIL, Bangalore. PBG should be from scheduled commercial bank (either private or PSU) buy not from any co-operative bank or NBFC. Bank guarantee (PBG) issued by a bank must be confirmed through the Structured Financial Messaging System (SFMS). If the issuing bank fails to send the SFMS message or if there are errors in the message, the PBG shall be rejected by RailTel.

4.10.4 In the case the bid is successful the PBG also will have to be submitted to RailTel on back-to-back basis.

4.10.4 In case work share arrangements are mutually agreed between RailTel and **Partner** then the PBG will be proportionately decided.

4.11 Last date & time for Submission of EOI response
EOI response should be submitted to RailTel as explained in the EOI document. The bids submitted after the specified date and time mentioned in the EOI will be summarily rejected.

4.12 Modification and/or Withdrawal of EOI response
EOI response once submitted will treated, as final and no modification will be permitted. No correspondence in this regard will be entertained.

No bidder shall be allowed to withdraw the response after the last date and time for submission. The successful bidder will not be allowed to withdraw or back out from the response commitments. In case of withdrawal or back out by the successful bidder, the

Earnest Money Deposit shall be forfeited, and all interests/claims of such **Partner** shall be deemed as foreclosed. In addition, if selected partner withdraws its offer, then the **Partner** may be blacklisted.

4.13 Details of Financial bid for the above referred tender

The final bid for the tender will be prepared jointly with the selected **Partner** for its respective portion so that RailTel puts in an optimal bid with a good chance of winning the Tender. Moreover, RailTel reserves the right for further negotiation and deduction in prices from the selected Service Partner to keep the RailTel's bid in winning position in the NSIL, BANGALORE tender.

4.14 Clarification of EOI Response

To assist in the examination, evaluation, and comparison of bids the purchaser may, at its discretion, ask the Service Partners 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.

4.15 Period of Association/Validity of Agreement

RailTel may enter into a pre-bid agreement with selected partner with detailed back-to-back Terms and conditions for respective selected portion of scope in each of the packages prior to submission of RailTel bid against NSIL, BANGALORE Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 and its corrigendum thereof.

5 Eligibility Criteria for Partners:

The bidders must comply with the following conditions for their eligibility in the participation for the EOI. Submit necessary declarations/certifications as per Tender Terms and Conditions:

Sl. No.	Parameter	Eligibility Criteria	Supporting Documents to be Submitted	Compliance (Y/N)
A)	**Association with RailTel**	The Bidder Should be RailTel's Empanelled Business Associates (BA) Business Partner (BP) with validity of association at least upto the last date of validity as cited in the customer's RFP bid. This is the primary and mandatory eligibility criteria; however, the bidder is also required to meet other eligibility criteria of this EOI. (Bidder who have already applied for the empanelment with RailTel before this EOI issuance date can also participate in the EOI. Proof of application and empanelment fee to RailTel shall be provided mandatorily in that case)	Copy of LOI/Agreement. Proof of application to be submitted.	
B)	**Financial Conditions**			
i)	**Company Registration**	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.	1. Certificate of Incorporation / Firm Registration 2. GST Registration 3. PAN Card	
ii)	**Average Annual Turnover**	a) The BA in the last three financial years i.e., 2021-22, 2022-23 & 2024-2025 (as on date of EOI) should have achieved a minimum	Turnover Certificate issued by the Statutory Auditors along with copy of the CA financial statements to be submitted.	

		average annual turnover of Rs.9,37,50,000. No exemption is allowed for MSME & Starup.	Audited P&L statements and Balance sheet and ITR for last consecutive 03 years. UDIN of the chartered accountant should be invariably be mentioned on the audited financial statements.	

iii)	**Positive Net worth**	Bidder should also have a positive net worth.	Positive Net Worth Certificate issued by the Statutory Auditors along with copy of the CA audited financial statements required.	

C)	**Technical Conditions**			
(i)	**Work experience**	The bidder must have executed similar work in last 7 years ending last day of month previous to the one in which EOI is invited. 1. One similar work of not less than the Value of 60% of the EOI. **OR** 2. Two similar works each of not less than the Value of 40% of the EOI. **OR** 3. Three similar works each of not less than Value of 30% of the EOI of estimated value of contract. Definition of similar work: Works entailing completion of Supply, Installation, Testing and Commissioning of a project in the field of IT/ICT/Telecom/ CCTV Security Surveillance/ Perimeter Security/NOC/SOC/Data Center/Cloud for any Government department or Public Sector Units or public listed companies/ State Govt. / PSU's / Govt. Bodies / Military Engineering Service/ Railways. Note: Ongoing works will be considered for value of completed work (minimum 70% work completion) certified by PO issuing authority / customer mentioning completed work value on the certificate along with satisfactory completion certificate for work completed so far. It shall be additional to above mentioned clause.	To this extent necessary PO copies/agreement copies / completion certificates. The information should also be submitted in the Annexure-XI. The copy of purchase order and installation certificates signed by the End user department clearly stating value of work completed and date of completion of work (against the PO issued) that the bidder has carried out installation of the said system to this effect must be submitted with the bid document. (Any prototype installation / test set-up or installation in bidder's or its affiliate premises will not be accepted). **For ongoing works**: Ongoing works will be considered for value of completed work (minimum 70% work completion) certified by PO issuing authority / customer mentioning completed work value on the certificate along with satisfactory completion certificate for work completed so far.	

(i)	**MAF**	The bidder needs to submit the documents required under MAF from the respective OEMs as part of the solution mentioning Back-to-Back arrangement, TAC support, End of Support.	MAF as per the Tender Document of **NSIL** Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025. The bidder is required to submit two number of MAFs as mentioned below: (i) The first MAF is required to be addressed to RailTel referring this subject EOI in favour of Bidder. (ii) The Second MAF is required to be addressed to **NSIL** referring **NSIL** tender and in favour of RailTel.	
(ii)	**PPLC - Purchase Preference Policy (linked with Local Content)**	Bidder shall comply with the clauses as per the Tender Document and the bidder must submit the compliance certificate for the same as per the Tender Document	Need to comply with NSIL tender requirements, if any.	
iii)	**Purchase Preference(pricing)**	No exemption is allowed for MSME & Startups under purchase preference for pricing.	Bidder will have to comply accordingly.	

A Copy of Purchase/Work Order & its Commissioning Certificate issued by Work Awarding Organization is to be submitted with EOI. Also, contact Details of concerned person i.e., Name/ Designation/Contact Number/Official Email ID, of the Work Awarding Organization needs to be mentioned.

For On-going projects, proof of satisfactory laying/part completion certificate for the desired quantity issued & signed by the competent authority of the client entity along with the supporting documents such as work order/purchase order clearly highlighting the scope of work, bill of material and value of the contract/ order.

a) "Similar Works" means **Installation and commissioning of IT Network Infrastructure including Access Level Layer 2/Layer 3 Switches or any related IT Systems with having obtained authorization from the OEM of the switches/router**.

b) Substantially completed works means those Works Which are at least 70% completed as on the date of tender submission (i.e gross value of Work done up to the last Date of Submission is 70% or more of the original contract price) and continuing satisfactorily.

c) Last seven (7) Years shall be counted from 28 days prior to the date of submission of Bid.

d) Completion certificates for works Issued by Private parties shall be Supported by TDS (Tax Deducted at Source) certificate.

6 Bidder's profile

The bidder shall provide the information in the below table:

Sl. No	ITEM	Details
1	Full name of bidder	
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, 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 **Schedule of Rates (SOR):** The bidder should quote as per the enclosed Annexure- I

8 Evaluation Criteria :

8.1 The **Partner** who fulfills the Eligibility criteria shall be further evaluated against the criteria mentioned in Annexure- II as applicable.

8.2 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.

8.3 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.

9 Payment terms

9.1 All payments shall be paid on back-to-back basis. RailTel shall make payment to selected **Partner** after receiving payment from Customer as per the Payment terms defined in the NSIL, Bangalore tender. In case of any penalty or deduction made by customer, same shall be passed on to partner if attributed to the **Partner**'s portion of Scope.

9.2 SLAs, LD, penalties levied by customer shall be applicable on back-to-back basis on prospective bidder on value terms **not on** percentage terms.

9.3 For payment terms of NSIL, Bangalore, bidders are advised to go the respective section of NSIL, Bangalore Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 and all its associated corrigendum/ addendum/clarifications.

10 Service Level Agreement

The selected bidder will be required to adhere to the SLA matrix as defined in the NSIL, Bangalore Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 for his scope of work and the SLA breach

penalty will be applicable proportionately on the selected bidder, as specified in the Tender. The SLA scoring and penalty deduction mechanism for in-scope of work area shall be followed as specified in the NSIL, Bangalore Tender. For payment terms of NSIL, Bangalore, bidders are advised to go to the respective section of NSIL, Bangalore Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025and all its associated corrigendum/addendum/ clarifications. 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.

11 Roles and Responsibility of the BA/SI Partner

The BA/SI will be responsible for the work as per scope of NSIL, Bangalore Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 and Corrigenda. The BA/SI should tightly integrate with OEM's solution providers and will provide manpower resources of this work. BA/SI should have sufficient backup support required for liasoning, meetings, coordination to meet the timelines of the project and its successful completion. The BA/SI shall nominate technical SPOC and account manager for this project.

The BA/SI should thoroughly study the RFP and Corrigendum floated by NSIL, Bangalore **for** compliance (enclosed).

A. Documentation: BA/SI shall prepare High Level Design doc (HLD) and Low-Level Design doc (LLD) as part of implementation of the project under EoI. Bidder shall be responsible for all the documentation/ reports required at various stages of project during the currency of the project.

B. Compliances: BA/SI shall be responsible for all the regulatory compliances related to fulfilment of delivery of this project under this EoI during its currency.

Above requirements are only indicative in nature and are only guidance of the bidder to assess the quantum of work. The BA/SI is required to apply their expertise to fulfil the required objective. In case of any discrepancy/typo-graphical error mentioned in this EoI then the conditions/specifications mentioned in the RFP & Corrigendum floated by NSIL, BANGALORE, will prevail.

C. Governance Framework:

- RailTel will setup a governance team comprising of RailTel & BA/SI. The team will have minimum of 2 member each from RailTel and BA/SI lead by GM/RailTel/SBC. The team size may increase if required based on approval of Competent Authority of RailTel.
- BA/SI shall deploy competent & experiences persons to be part of the governance team.
- The BA/SI shall comply with all the ITIL processes and shall be responsible for its implementation across the various activities and deliverables against the scope of the project.
- The BA/SI shall adhere to the governance framework put in by RailTel for the project deliverables.
- The Governance team among the other things will monitor the performance of the project and take corrective measures as required for successful delivery of the project.

The Governance Team shall be overseeing the coordination, periodical reviews, escalations, billing, documentation, customer interactions etc.

12. Arbitration

The parties through respective signatories shall settle any dispute or disagreement with respect to performance, non-performance, or defective performance of respective obligation amicably. In the event of disputes remaining unresolved, the parties shall refer the matter to a single arbitrator under arbitration law that may be applicable, whose appointment shall be done by CMD, RailTel Corporation of India Limited. The place of arbitration shall be New Delhi and the language used shall be English.

13. Force Majeure Clause

If at any time, during the continuance of this contract, the performance, in whole or part, by either party, of any obligation under this contract shall be prevented or delayed by reason of any war, hostility, act of the public enemy, Civil Commotion, Sabotage, Fires, Floods, Earthquakes, explosions, strikes, epidemics, quarantine restrictions, lockouts, any statute, statutory rules/regulations, order of requisitions issued by any Government Department or Competent Authority of acts of God (here-in-after referred to as event)then provided notice of the happening of any such event is given by either party to the other within twenty one days from the date of occurrence thereof ,neither party shall, by reason of such event, be entitled to terminate this Contract nor shall either party have any claim for damage against the other in respect of such non-performance or delay in performance, and the obligations under the Contract shall be resumed as soon as practicable after such event has come to an end or ceased to exist, PROVIDED FURTHER that if the performance in whole or part of any obligation under this Contract is prevented or delayed by reason of any such event beyond a period as mutually agreed to by the RailTel and the Contract or after any event or 60days in the absence of such an agreement which ever is more, either party may at its option terminate the Contract provided also that if the contract is so terminated under this clause the RailTel may at the time of such termination take over from the Contractor at prices as provided for in the contract ,all works executed or works under execution.

14. Integrity pact:

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

b) Only those vendors who have purchased the tender document and signed the IP document can send their grievances, if any, to the Independent External Monitors (IEMs) through the nodal officer, GM (Admin & Security)/CO RailTel.

Name of IEMs and contact details:

i) Shri. Vinit Kumar Jayaswal,
Add: E-34, Brahma Apartments, Plot-7,
Sector-7, Dwarka, New Delhi-110075.
E-Mail: gkvinit@gmail.com
M.No. +91-9871893484

ii) Shri. Punati Sridhar,
Add: 8C, Block 4, 14-C Cross, MCHS Colony, HSR 6th Sector, Bangaluru-560102.

E-Mail: poonatis@gmail.com
M.No. +91-9448105097

iii) Shri. Bipin Bihari Mallick,
Add: HIG 11, Kalinga Vihar,
Kalinga Nagar K5, Subudhipur,
Bhubaneswar, Odisha, 751019.
E-Mail: bipinmallick@gmail.com
M.No. +91-9968150900

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

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

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

f) **The 'Integrity Pact' shall be submitted by the Bidder duly signed in all pages along with the Bid in a separate envelope, duly superscripted with 'Integrity Pact'. Tender received without signed copy of the Integrity Pact document will be liable to be rejected. Proforma for signing the Integrity Pact is available in Chapter-6 of this tender document (Form No. 6).**

g) One copy of the Integrity Pact shall be retained by RailTel (RCIL) and the 2nd copy will be issued to the representative of the bidders during bid opening. If the Bidders representative is not present during the Bid opening, the 2nd copy shall be sent to the bidder by post/courier.

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

The bidder shall submit the signed Integrity Pact (2 Copies) as per Annexure – XI

Note :

1) All the terms & conditions of NSIL, Bangalore including Scope of work, ITT, GTC, Payments, SLA & Penalties, warranty etc., shall be complied with by all bidders and applicable on back-back basis with the successful partner. Entire work shall be completed in all respects within 06 months from the date of issue of LoI/LoA/PO/SO from this office.

2) The tender document of NSIL, Bangalore is placed at the end of this EoI.

3) All the documents must be submitted with proper indexing with page numbers & signed.

=====


रेलटेल
RAILTEL

Annexure - I : Schedule of Requirement & Technical specification

Name of Work:

"SUPPLY, INSTALLATION, COMMISSIONING, OPERATION AND MAINTENANCE OF UPGRADATION OF IT INFRASTRUCTURE:

List of deliverables/ items / service required along with technical specification for hardware and services, which is required to be delivered as part of the scope is as follows:-

Ser	Description	Qty	Technical Spec / Requirement*
1	Workstation	54	Appendix 'A'
2	Monitor	74	Appendix 'B'
3	NAS Storage (250 TB)	1	Appendix 'C'
4	Tape Backup	1	
5	Server (Rack) - Config-1	24	Appendix 'D'
6	Edge Switch	32	Appendix 'E'
7	Core Switch	2	Appendix 'F'
8	UTM/NGFW-Config-1	2	Appendix 'G'
	UTM/ NGFW - Config-2	6	
	UTM Hardware Authentication Token	20	
9	NGFW Logger & Traffic Analyser	1	
10	NGFW Manager	1	
11	End Point Protection & Management Tool	150	
12	Interconnect Router - Config-1	2	Appendix 'H'
13	Interconnect Router - Config-2	4	
14	Server Room Structured Cabling and Accessories	1	Appendix 'I'

15	All-in-one PC	6	Appendix 'J'
16	NMS Laptop	2	Appendix 'K'
17	ATS Device	8	Appendix 'L'
18	STC Server Node	8	Appendix 'M'
19	MCP Server	6	Appendix 'N'
20	Thin Client AIO	14	Appendix 'M' & 'N'
21	LCD Display with Trolley / Wall mount (75 inch)	3	Appendix 'O'
22	Syslog Servers - Config-2	5	Appendix 'P'
23	SIEM Server/ Security Analytics Server - Config-3	3	Appendix 'Q'
24	Printer - Color	2	Appendix 'R'
25	Printer - BW	8	Appendix 'S'
26	NMS Software with Lics	1	Appendix 'T'
27	RKM	8	Appendix 'U'
28	KVM (40 Port) - Config-1	1	
	KVM (8 Port) - Config-2	2	
29	SIEM Software with 3500 EPS	1	Appendix 'V'
30	Network Behavior Analytics (NBA/NBAD)		Appendix 'W'
31	One Time Implementation + Documentation	1	Appendix 'X'
32	UT Display	24	Appendix 'Y'
33	Onsite Support - 2 Skills	For warranty and CAMC period	Appendix 'Z'
34	Onsite Support - Security Service - 1 Skill	For warranty and CAMC period	
35	Windows Server OS 2022	6	

36	Other Technical Terms and Conditions		Appendix 'AA'

The table above "List of Deliverables" (not exhaustive), list "include major deliverables for Upgradation of IT Infrastructure system, but are not limited to,". Bidder to note that the offer needs to include all the items required to realize the IT Infrastructure as per the required configuration and specification.

*The detailed Appendices are in the following section.

Detailed Specifications of Deliverables

This chapter contains detailed technical specification of all the deliverables.

1. Appendix 'A' - Workstations

Workstation shall be as per the specifications below:

a. Tower model, RHEL & Windows certified hardware. All the required device drivers for RHEL shall be included in the offer. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

b. **Physical dimension –** The dimension of the workstation (without monitor) shall be strictly within 210 mm x 485 mm x 520mm (W X D X H).

c. **Processor –** One CPU equivalent or better - Intel® Xeon® W5-2465X (16C 3.1 GHz, HT 33.75 MB 200W) or AMD on X86_64 architecture with equivalent or better specification.

d. **Memory -** 128 GB DDR4-2133 ECC Registered memory spread across all memory channels or better configuration

e. **Graphics -** NVIDIA T400 2GB GDDR6 or better. Drivers shall be delivered for RHEL.

f. **Drive Controller –** SAS/SATA controller with Raid 1

g. **Internal Storage –** 2 x 1TB Enterprise SATA HDD in RAID 1 configuration or better shall be offered. HDD shall not be returned back during warranty replacement. DMR to be provided.

h. **Network Controller –** Two independent PCIe network adaptor cards each with dual gigabit Ethernet shall be offered (total 2x2 = 4 nos ports) in addition to the integrated network adaptor port on the motherboard

i. USB keyboard and USB optical mouse to be offered.

j. **Optical Drive –** Internal DVD RW drive

k. Offered workstation shall support dual monitor configuration. Required video cables and / convertors to be offered along with the monitor. All the cables and converters shall be OEM certified component.

l. **Ports –** Front :2 USB, Rear: 4 USB, Audio in, out and Microphone

m. The system shall have integrated sound card and shall have internal Speaker. Should have required multimedia drivers pre-installed.

n. Tool less access to access panel, optical drive, hard drives, expansion cards, processor sockets, memory and internal cables and connectors.

o. **Cooling –** Shall be configured with cooling fans for Power supply, CPU heat sink, and chassis rear or chassis front.

p. **Power–** Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

q. **Certifications –** Following or equivalent international certification are to be provided along with the hardware:

   i. RoHS India [E-Waste (Management) Rules, 2016] certification

   ii. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

   iii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

   iv. Security Compliance – TPM 2.0, UEFI Secure boot

r. **Operating System –** Redhat Enterprise Linux (OEM package of RHEL latest version) Workstation edition to be provided pre-installed in all workstations with three years.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

2. Appendix 'B' - Monitor Specifications

Monitor shall be from same OEM make as of the workstations, the minimum hardware specifications for the monitor is as mentioned below:-

a. 27 Inches (27 inch or 68.5 cm diagonal viewable image size) Monitor

b. Panel Type/ Surface: IPS, LED backlight, antiglare display

c. **Aspect Ratio:** 16:9

d. **Viewing angle:** Upto 178/ 178

e. **Brightness:** upto 350 cd/m2

f. **Contrast Ratio:** Static – 1000:1 static; 2000000:1 dynamic

g. Response Time: 8ms

h. **Pixel Pitch:** 0.233 mm

i. **Color Depth:** 16.7 Million

j. **Native Resolution:** 2560 x 1440

k. **Interface:** Compatible with the offered workstation model suitable to drive dual display configuration.

l. Support for Tilt, Swivel and Pivot rotation

m. Support for VESA mount

n. Each monitor shall be offered with USB powered integrated speaker bar which shall be seamlessly attaches to the monitor's bezel.

o. Power Supply rating: AC 120/230 V (50/60 Hz)

p. Required video cables / convertors along with the monitor. All cables and convertors shall be OEM certified hardware

s. Monitor to be certified with following or equivalent international certification

   i. RoHS India [E-Waste (Management) Rules, 2016] certification

   ii. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

   iii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

3. Appendix 'C' - NAS Storage and Backup Infrastructure

Storage shall consist of the following items and as per the specifications detailed below for each item:

No.	Item	Quantity
a.	High Available NAS 250 TB	1 nos
b.	Backup Software (host-based license)	1 nos
c.	Tape Library with Media	1 nos
d.	Backup Server	1 nos
e.	SAN Switch	1 nos

a. High Available NAS

The NAS should offer Unified Storage which supports out of the box capability for different storage protocol under a single management console. The NAS solution offered should be the same product family of a single manufacturer. The storage controller shall be licensed for partitioning / virtual controller / feature for multitenant environment. The Unified Storage Operating System should be owned by the Storage Hardware Manufacturer. The NAS should have High Availability features as mentioned below:

i. The offered solution should be configured with no single point of failure (NSPoF).

ii. The offered solution should be configured with dual controllers which supports Active-Active mode.

iii. The offered solution should provide session/cache information replication across the controllers to support faster failover across the controllers.

iv. It should retain the state information of the active transactions during a controller failover event.

v. Any maintenance activity on the storage, controller OS upgradation, and file system expansion should be performed online without downtime.

vi. Any maintenance activity should be non-destructive for the stored data.

vii. During controller failover shall complete well with in before the client nodes detect file system or storage block is unavailable. Storage which requires remounting of file system or block storage during controller failover event should not be offered.

viii. The NAS configuration should not result in single point of failure at any stage / part failure. Adequate redundancy to be incorporated in the hardware to cater for sustained operations in case of any part failure.

ix. **Physical.** 19 inch Rack mountable Storage hardware along with rack mount kit shall be provided. Such enclosure should permit maintenance access to the subsystems / cards inside without requiring dismounting from the rack.

x. **Protocol Support.** The storage controller should be offered with NFS (v3, v4, v4.1 support), FC, CIFS & iSCSI protocol support. If any additional hardware software is required to support all the required protocol then should be offered in redundancy to ensure NSPoF.

xi. **Disk Enclosure.** The Disk enclosures shall be offered with sufficient capacity to house required number of disks. Specification of the disk enclosure is as mentioned below:

1) The disks offered should be 12Gbps dual ported drives
2) The disk enclosure shall be configured with required interconnection cables to have connectivity with both the controller to avoid single point of failure.
3) The disk enclosure shall be configured with hot swappable redundant power supply and fan tray
4) The usable storage capacity of 250 TB at the file system level should be offered. The offered capacity shall have 230 TB NL-SAS and 20 TB on SSD.
5) Vendor should note that the capacity mentioned above is the usable/workable capacity at the file system level. Vendor should quote for appropriate configuration considering the spares and RAID configuration. For NL-SAS Drive, vendor should consider maximum 12 drives in a RAID group offering 3 disk protection per RAID group. If the solution does not offer 3 Disk protection capability, the solution should be designed with equivalent numbers of disks in global hot spare. The detailed breakup on the disk count to be provided along with the proposal. For NL-SAS drive two global hot spare drive to be offered.
6) The SSD pool can be offered on RAID 6 or on RAID 1 with two global hot spare.
7) Vendor should demonstrate the usable capacity on a Linux NFS client using standard Linux commands like "du -sh".
8) A detailed calculation in arriving at the number of disks to meet the usable storage requirement of 250 TB should be provided along with the offer considering all the penalty in disk group, volume and RAID configuration.
9) Vendor shall include 20% of disk space as file system snapshot reserve area in the file system calculation. The usable capacity shall be derived excluding snapshot reserve area in the file system. Hence 250 TB usable

file system shall have additional 20% disk space reserved/dedicated for snapshot.

10) The storage enclosure shall be populated with **maximum 16 TB Enterprise NL-SAS** and **maximum 4 TB SSD** as performance drive. The vendor can offer lower capacity disk.

11) If vendor is offering higher capacity disk than specified above the total number of disk count shall be as per **16 TB NL SAS and 4TB SSD disk**. Vendor has to offer disks counts accordingly and licenses shall be extended for full capacity.

xii. **Scalability.**

1) The offered storage controller shall be scalable up to 400 drives in a single pair of controllers.

2) The unified proposed system should be field upgradeable to a higher model through data-in-place upgrades

xiii. **Defense against Malware / Ransomware attack.**

1) Product shall offer WORM feature which can be configured on specific volume based on requirement

2) The product shall have capability to block writing malicious files on the disk. Suitable license and configuration to be offered.

3) The product shall have capability to monitor infrastructure for ransom ware attack.

4) The product shall have capability to generate alert for suspicious activity

xiv. **Storage Solution Features and Architecture**

1) The unified storage architecture should be based upon dedicated appliance, running specialized operating system optimized for storage operations.

2) The host operating system in the controller should be strictly based on Unix/Linux based kernel with a specialized environment built to support high performance file service. The storage operating system should not be based on general purpose OS.

3) The proposed Unified storage architecture should not be based upon file services running on general purpose OS and conventional server hardware.

4) The storage should be able to provide single name space/file system for configured capacity and should be scalable upto 256 TB

5) The controller unified storage operating system should be protected by RAID.

6) The controller should support creating disk groups in different RAID levels viz., mirroring, single parity and dual parity or equivalent data protection technologies

7) Each controller should be configured with at least 32 GB of memory.

8) The system should be configured with minimum 4 TB of SSD/Flash/NVMe based cache for accelerating the performance. This SSD or NVMe based pool will not be part of file system.

9) Storage Controller should be capable of supporting a single LUN of size of at least 16 TB.

10) Controllers should support different disk drives viz., SSD, SAS, NL-SAS.

11) It should be possible to grow the file system online.

12) It should be possible to grow the disk pool online to grow the file system.

13) The storage should support data tiering with movement of hot data to high performing drives. It should offer the capability to move data between one tier of drives to another tier of drives.

14) The controller cache should support battery backup option or equivalent technology to protect uncommitted data against power failure.

15) The controller should be configured for point in time images or snapshots and applicable licensing should be offered. It should be possible to take at least 64 snapshots per file system.

16) Proposed storage shall support post process deduplication and compress on SSD tier.

17) The proposed storage array must support data at rest encryption offering industry standard certification/compliance. The storage array may implement data at rest encryption using self-encrypting drives or controller-based functionality there by not impacting performance.

18) The controller should have DE-duplication & compression features for file system access and necessary licensing for the offered solution should be included.

19) It should be possible to configure quotas on the user, volume and directory level.

20) Storage controller shall support NDMP for backup and restore operation.

21) Shall support LDAP and Active Directory integration

xv. **Management Software**

1) The software for managing the storage device should be Web GUI based or CLI.
2) The storage should have out-of-band management feature on Ethernet.
3) Storage administrator console shall be protected by multi-factor authentication
4) The proposed management interface should be able to manage, configure and monitor the environment.
5) Single management, easy to use GUI based and web enabled administration interface for configuration, storage management and performance analysis tools for both block and file.
6) The interface shall allow to manage the entire storage solution from single interface which allows - Storage Management, Cluster Management, DR Configuration Management.
7) The management console shall allow to generate reports on block and file access for a given duration for per node, per user, per volume on a specific administrative domain.
8) On-premise performance analysis, workload planning should be supported

xvi. **Audit Trail Capability.** The Storage solution shall offer suitable solution to retain detailed of NFS Transaction Log to record every file access on the shared file system. The audit log shall include access time stamp, client node IP, mode of access (read or write) and user information. This log shall be retained at least for last 72 hours and shall be in searchable format. Vendor shall offer required resources for capturing this information.

xvii. **Power Requirement.** The offered storage solution should be supplied with hot swappable redundant power supply units, for all the components (Storage Controller, desk Shelves) wherever provision exists in addition to No Single Point of Failure clause mentioned earlier.

1) Power Supply rating: 220 volt/50 Hz.
2) Required power cable shall be offered with the storage.

xviii. **Interfaces / Ports per Controller**

1) Each storage controller should be configured following network ports:
   i. 1G Copper Ethernet - 2 Nos
   ii. 10 G Fiber Ethernet (10 G SR LC Type) – 4 Nos
2) Link aggregation/ trunking of the Ethernet ports should be supported.
3) FC Port – Each storage controller should also be configured with two 16 Gb FC port with transceiver (SR type) for connecting to the SAN switch for backup and for providing block access.

4) Required network cables and FC cables to be offered.

xix. **Performance.** The offered storage controller (each controller) shall support minimum throughput of 50000 IOPS at 8K block size with NFS. Bandwidth – 1.6 GBps with 32 K block size at 80% read and 20% write with NFS.

xx. **Compliance & Certification.** The offered product must be complaint to following certification or equivalent global certification –

1) RoHS India [E-Waste (Management) Rules, 2016] certification Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard
2) Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer/ Hardware.
3) Valid Indian Common Criteria Certification Scheme (IC3S) for EAL2 or better for the offer product or offered version of firmware.

xxi. **POC Requirement**

1) The vendor/OEM shall offer similar storage product in remote access mode over Internet for NSIL to evaluate the features of the offered product during technical evaluation of the offer wherever NSIL request for such POC to the vendor.
2) The offered product for evaluation shall be on offered product line with similar storage operating system version with required licenses.
3) If multiple vendors offer same OEM product on similar BOM, a single remote access offered directly from OEM shall be asked for evaluation of the product
4) NSIL will need access to the storage product for management console and two NFS clients and two SAN client on the network to evaluate the product features.
5) Vendor shall ensure NSIL has remote access to storage controller management console, storage controller logs, client device and logs. NSIL shall evaluate high availability feature, multi-tenancy feature etc. for the product and suitable configuration shall be offered.
6) NSIL will communicate to the Vendor on specific feature sets which NSIL would like to evaluate on the offered product. The selection of the specific product features will be decided by Competent Authority during the technical evaluation process.
7) NSIL will decide the demonstration requirement of feature sets across

OEM products and the requirement will vary based on OEM product.

8) Vendor shall assist NSIL team in configuration and demonstration of product features.

9) Vendor shall keep all the required resource ready for remote evaluation during quoting for this tender. The remote lab configuration diagram, access credentials and access methods shall be shared along with the technical offer. The vendor shall enable remote access immediately after receipt of the email communication via NSIL purchase.

10) In case the vendor or OEM is not able to successful demonstration of the feature with-in two weeks' time after receipt of the requirement, NSIL will not accept any further request for extension or re-evaluation of the feature demonstration activity.

11) The outcome of the feature demonstration will be based on the decision of the NSIL Purchase.

b. Backup Software (host-based license)

i. **Backup Solution Architecture**

1) The backup software should be offered on RHEL platform. Backup Software offered should be compatible with offered RHEL version on Backup Server.

2) Backup/restore software architecture should assure continuity of backup/restore operations even under the failure of one of the nodes involved in the backup/restore (i.e. NAS filer/file server nodes)

3) The backup / restore solution should permit multiple copies of the backups to be maintained including the support for offline vaulting of one or more copies

4) It shall be possible to take tape backups for the following:
   - a file
   - a directory
   - a directory structure
   - an entire volume
   - any snapshot copy

5) The following backup options shall be supported:
   - Full backup
   - Incremental backup
   - Differential Backup

6) The administration facility should be provided using a suitable easy-to- use GUI to centrally monitor and administer the backup environment.

7) It should also be possible to manage & administer backup environment using command line Interface.

8) The backup software should be capable to perform policy based automated backup scheduled based on calendar schedule (specific day, week, month).

9) The backup software should have options to choose the following features:
   - Backup Window
   - Backup Retry
   - Backup Source
   - Backup Media Pool

10) The backup software should have option to take backup of entire backup configuration and catalog data

11) It should be possible to restore the following:
   - Full File System.
   - Selected Directories.
   - Selected file/s

12) Proposed solution must include safeguards against ransomware attacks or intentional deletion of backup data by malicious actors who exploit compromised authentication on the backup server or software. Access to data in recovery scenarios must be restricted to "Recovery Admin" or "Super Admin" roles, and this access should be secured through dedicated local authentication, segmented business user access, or Multi-Factor Authentication (MFA) utilizing SAML or integration with third- party solutions such as OneLogin, Azure, and Okta etc.

13) Proposed backup solution should strengthen the defenses against ransomware and other cyber-attacks with features including: immutable backups, ransomware recovery, object storage locking, cloud tiering with data locking, data encryption, multi-factor authentication, restricted backup storage protocol for Storing all critical backups

ii. **License Requirement**

1) The offered backup solution should have host based NDMP or dual socket license for taking NDMP backup of the NAS storage for full volume without NAS capacity limitations

2) Software shall support both direct and 3 way NDMP Backup.

3) Offered Solution must support Browsable Volume Selection and Direct Access Restore(DAR) for Backups from the Tape to NAS Mount Point, which enables fast recovery of whole directories, single files, or subsets of files by recording each file's location within the backup media and should avoid sequential-read through the entire backup set for faster restoration

4) Offered Solution must support Incremental Restore for specific backup

data

5) Offered Solution must support Dynamic Drive Sharing on SAN Tape Drives between NAS devices (Filers) / Backup Server / SAN Clients and Operate seamlessly between multiple platforms

6) The backup solution should be offered with 2 numbers of network client with single socket count license in Linux platform.

iii. **Backup Management Feature**

1) It should be possible to restore the contents of the media on a system different from the one on which the backup was taken

2) It should provide a user-friendly enterprise console that enables the administrator to manage the complete backup and recovery environment via a Web-based interface

3) The proposed backup solution should allow search capability enables fast and granular searches of its backup index for backup and restore. Include fast-search capabilities for metadata (name, modified date, type, etc.) and save-sets with offline indexes in your search results

4) Backup Solution must have Single sign-on (SSO) features to Log into Backup Software using AD/LDAP credentials along with Role-based access control to regulates operations administrators

c. Tape Library -

i. 19-inch Rack Mountable – 3U/4U Tape library.

ii. The tape library should be configured with two LTO9 tape drives. All the drives must be Dual Port LTO9 FC Drives. The LTO 9 Drive FC interface shall be compatible with offered SAN switch.

iii. The number of slots for tape media should be minimum 40 Slots usable/Licensed, without Stacking modules.

iv. The tape library should support minimum five mail slots.

v. The tape library should be with two or more magazine configuration.

vi. The tape library should support both read and write operations of LTO9 media.

vii. Offered LTO9 drives in the Library shall conform to the Continuous and Data rate matching technique for higher reliability.

viii. Offered Tape Library shall have partitioning support so that each drive can be configured in a separate partition. Required license shall be offered.

ix. The tape library should have a GUI panel & also should be manageable remotely from web-based GUI.

x. It should be possible to manage the following using both local & remote management - Moving media, Load/unload tape drives, Access to the diagnostics, Library configurations, Library statistics, Inventory check.

xi. The tape library native capacity should be minimum 720TB Native and 1.8 PB (compressed 2.5:1). Required license shall be offered.

xii. The tape library transfer rate should be 3.24 TB/Hr (native) in fully loaded configuration (3 Drive configuration).

xiii. MSBF (Mean Swaps Between Failures) >= 1 Million Robot load/unload cycles or MTBF of 125,000 Hours.

xiv. Native Transfer Rate: > = Shall support full throughput from all the drives operating concurrently at their maximum transfer rates.

xv. The Tape Library should have FC interconnect to the SAN switch to enable NDMP backup and restore operations.

xvi. The Tape Library should support taking backup over NDMP.

xvii. The offered tape library should be configured with Field Replaceable Tape Drives, Magazines, Power Supply Units

xviii. The Tape Library should have barcode reader feature for media management. Required number of Barcodes shall be included in the offer.

xix. Proactive Diagnostics: Proactive monitoring feature within the library to monitor major subsystems, run self-diagnostic procedures, and send policy- based communications to system administrators

xx. Support for auto clean feature

xxi. Encryption capability - AES 256-bit

xxii. Dedicated management port for remote management of Library

xxiii. Number of LTO9 Tape Media to be offered = 70

xxiv. Number of cleaning cartridges to be offered =10

xxv. Hot Pluggable redundant power supply, 80 plus rating

xxvi. Regulatory Ratings –

- Safety: IEC-60950 with worldwide country deviations with Class 1 Laser product
- Emissions Standards: FCC Class A or equivalent Indian standard
- ROHS or ROHS India

d. <u>Backup Server</u>

i. **Physical** – 19-ich rack mountable server of 2U rack mount size. Servers shall be offered with required rack mount hardware kit.

ii. **Processor** – single processor with minimum 16 cores and 2.4 Ghz clock or better

processor (Intel or AMD).

iii. **Memory** - 96 GB Memory in best deployable model

iv. Internal Storage Hot pluggable HDD: 2 Nos of 1.92 TB Mix Use Hot Pluggable SSD with DWPD >= 1.0 in RAID 1

v. **Drive Bay** – Server shall support 4 Hot-Plug Hard disk drive Bay

vi. The server must be RHEL certified hardware and listed in RHEL portal.

vii. **Drive Controller** – 12G SAS controller with RAID 1.

viii. **Optical Drive** – Internal DVD RW drive to be offered

ix. **Network Controller** – Two 1G Ethernet port and four 10G Ethernet ports

x. **HBA Port** - The server should be configured with two numbers of 16Gb FC HBA cards for connecting to the SAN switch. Vendor should offer multipath driver for HBA

xi. **Ports** – Front :2 USB, Rear: 4 USB, VGA=1

xii. **Power** – Hot Pluggable redundant power supply. Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

xiii. **Management** - Server shall include IPMI 2.0 compliant management module . Management function shall be offered on out of band over Ethernet.

xiv. Management functionalities (viz., power off, power on, reboot, System health monitoring, remote media mount and software installation) should be possible to be carried out using the offered management module.

xv. **Cooling** – Server shall be configured with redundant cooling fans.

xvi. **Certifications** – Following or equivalent international certification

(a) RoHS India [E-Waste (Management) Rules, 2016] certification
(b) Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard
(c) Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

xvii. If the offered backup software requires a better configuration, the required hardware should be offered.

e. <u>SAN Switch</u>

i. Vendor has to offer SAN Switches with the following specifications:

ii. 16 Gb FC ports = 12 nos

iii. Non-blocking wire speed performance for all ports. i.e. minimum 384 Gbps of switch bandwidth

iv. Required FC transceivers should be included.

v. 12 nos of 5 meter FC cables should be offered.

vi. Should be offered with ISL trunking license

vii. Class of service: Class 2, Class 3, and Class F

viii. Supported fabric services - Name server, Registered state change notification (RSCN), Login services, Public loop, Broadcast, In-order delivery, Name-server zoning, NTP.

ix. Supported diagnostics features - Power-on self-test (POST) diagnostics, Online diagnostics, Fiber Channel traceroute capability, Fiber Channel ping and debug, Syslog, Port-level statistics.

x. Should be offered with zoning (default zoning, port/WWN zoning, broadcast zoning) and VSAN licenses.

xi. Supported management features - HTTP, SNMP V1/V3, SSH

xii. Should be configured with dual hot swappable power supply

xiii. Should be configured with adequate cooling fans.

xiv. Should support out of band management over Ethernet.

xv. Should support configuration and management over web console.

xvi. 19 inch rack mountable with rack mount kit.

xvii. Compliance – CB, WEEE, ROHS

f. Installation & Commissioning –

i. Vendor shall provide required FC interconnection cables for integration of SAN switch, Tape Library, Backup Server and Storage.

ii. Vendor shall implement NDMP LAN Free backup and make suitable interconnect and policy configuration.

iii. Vendor shall provide four numbers of 10 meter FC cables for interconnecting NAS 10G ports with LAN switches.

iv. Vendor shall provide required number of FC cables for interconnecting Tape Library, SAN switch and Storage HBA ports during installation.

v. Vendor should provide detailed documentation on storage solution acceptance and implementation as a part of solution implementation activity.

vi. Vendor shall depute certified engineer on Storage and backup environment to carry out the acceptance and implementation at Bhopal.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

4. Appendix 'D' - RACK Servers

1. Specifications for Rack Server – Configuration – 1:

a. **Physical** – 19-inch rack mountable server of 1U rack mount size. Servers shall be offered with required rack mount hardware kit.

b. **Processor** – One Intel® Xeon® Gold 6548N Processor (60M cache, 32 Cores, 64 Threads, 2.80 GHz) or better or equivalent AMD processor on X86-64 architecture.

c. **Memory** - 128 GB ECC memory spread across all memory channels or better memory configuration.

d. **Internal Storage** – 6 Nos of 1.92TB SAS 12G Mixed Use SFF SSD Drive Writes Per Day (DWPD) > = 1

e. **Drive Controller** – Internal RAID Card for RAID 1, 0, 10, 5 and 6 support with 8 GB Memory

f. **OS Certification** - RHEL & Windows certified hardware. All the required device drivers for RHEL shall be included in the offer. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

g. **Optical Drive** – Internal DVD RW drive to be offered

h. **Network Controller** – Total 4 nos of 1Gb Ethernet copper and four numbers of 10Gb Ethernet Copper port shall be configured for each server.

i. **Ports** – Front :2 USB, Rear: 4 USB, VGA=1

j. **Power** –Hot Pluggable redundant power supply. Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

k. **Management** - Server shall include IPMI 2.0 compliant management module . Management function shall be offered on out of band over Ethernet.

l. **Cooling** – Server shall be configured with redundant cooling fans.

m. **Certifications** – Following or equivalent international certification

- RoHS India [E-Waste (Management) Rules, 2016] certification
- Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard
- Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer
- Security Compliance – TPM 2.0, UEFI Secure boot

q. **Support for Proxmox VE** – The offered server platform shall be compatible with Proxmox VE HCI solution. If the solution is not compatible to Proxmox, then vendor need to quote for equivalent HCI license for 3 clusters each with minimum 3 node

and each Cluster shall host 10 VMs. The CPU core, disk and memory support shall be as per offered server configuration. The HCI platform shall have OEM support during the support period for upgrade and bug fixes. The vendor also need to ensure implementation of the cluster as per implementation requirement described in the subsequent section.

r. **Operating System– RedHat Enterprise Linux 9.x or latest:** EIGHT nos of 2 socket licenses with 7 years support to be provided.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

5. Appendix 'E' – Edge Switches

Specifications for Edge Switch (Mission) (24 Port):

a. **Physical.** 19-inch rack mountable chassis along with rack mount kit. Offered switch shall be within 2U form factor.

b. Port Requirement:

i. Switch shall have at least 24 nos. of 10/100/1000 Base-T ports and additionally at least 4 nos. of 1/10 Gbps SFP Gbps SFP+ uplink ports (SX/LX).

ii. The Switch shall be configured with 2 nos. of 1000 BaseLX transceivers (out of the four combo ports mentioned above) to support minimum upto 10 KM.

iii. The transceivers offered should be from the same switch manufacturer (OEM) only.

iv. Switch should have dedicated slot for modular stacking, in addition to asked uplink ports.

v. Required stacking cable (3 Meter) shall be delivered with each switch

c. **Scalability requirement.** Offered switch should capable to support a future upgrade to 2 * 25Gbps uplink module.

d. Performance

i. Minimum Switching capacity 148 Gbps (Excluding Stacking Bandwidth)

ii. Minimum Throughput 110 million pps (Excluding Stacking Bandwidth)

iii. Offered switch shall be fully non-blocking architecture

iv. The configuration for an individual switch shall be realized using a single chassis (not by stacking)

e. General Feature –

i. **Trunking**: Maximum ports per trunk: 8, Maximum trunk groups: 4

ii. The offered switches shall be hardware ready for SDN support

iii. Support for PTP and NTP

iv. Switch shall offer open flow V1.0/V1.3 or equivalent.

f. Layer 2 Features –

i. VLAN support and tagging

ii. 802.1s Multiple Spanning Tree Protocol
iii. 802.1X Authentication
iv. MAC-Layer Filtering
v. Port Security - MAC Learning Disable
vi. Jumbo packet support, Max Size=9000 Bytes
vii. Rapid Per-VLAN Spanning Tree (RPVST+)

g. Layer -3 Features –

i. VRF / VRF-lite
ii. BGP, OSPF and IS-IS Routing
iii. VRRP/VRRP-E/HSRP
iv. Multicast Routing
v. Generic Routing Encapsulation (GRE)
vi. Switch should support minimum 16 VRF instances with route leaking functionality
vii. Switch should be able to support sub-interfaces
viii. Switch should support open standards based EVPN to support VXLAN based overlay network for layer-2 (VLAN) and layer-3 (VRF) extension.
ix. The Switch should support 10k IPv4 LPM (Longest Prefix Match) routes
x. Support for port mirroring on L3 network
xi. Static and Dynamic NAT

h. IPV6 Support –

i. IPv6 host support at the edge network
ii. IPv6 Routing (OSPF v3),BGP4+ (IPv6)
iii. VRF (IPv6)
iv. IPv6 over IPv4 tunnels
v. Multicast Listener Discovery (MLD) version 2 snooping

i. Security Features –

i. 802.1x Accounting
ii. MAC Authentication

iii. Protection against Denial of Service (DoS) attacks

iv. Encryption -- Must support 128-bit Advanced Encryption Standard (AES) for SSL/Management encrypted traffic

v. ACL - Provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number

vi. MACSEC

j. Supported Protocol and RFC Standards-

i. 802.1D Bridging

ii. 802.1q VLAN Tagging

iii. 802.1p Mapping to Priority Queue

iv. 802.1w Rapid Spanning Tree (RSTP)

v. 802.3ad Link Aggregation

vi. 802.3x Flow Control

vii. SNMP V1, V2, V3

viii. RFC 783 TFTP

ix. RFC 854 Telnet

x. RFC 1757 RMON MIB

xi. RFC 896 Congestion Control in IP/TCP Internetworks

xii. RFC 950 Internet Standard Sub-netting Procedure

xiii. RFC 1191 Path MTU Discovery

xiv. RFC 1403 BGP OSPF Interaction

xv. RFC 1519 Classless Inter-Domain Routing (CIDR):

xvi. RFC 1812 Requirements for IP Version 4 Routers

xvii. RFC 2236 Internet Group Management Protocol (IGMP) Version 2

xviii. RFC 1887 An Architecture for IPv6 Unicast Address Allocation

xix. RFC 1981 Path MTU Discovery for IPv6

xx. RFC 2374 IPv6 Aggregatable Global Unicast Address Format

xxi. RFC 2373 IPv6 Addressing Architecture

xxii. RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)

xxiii. RFC 5308 Routing IPv6 with IS-IS

xxiv. RFC 7348- Virtual extensible Local Area Network (VxLAN)

xxv. RFC 1349 Use of OSI IS-IS for routing in TCP/IP and dual environments

xxvi. OEM can refer to updated or equivalent RFC wherever applicable

k. Power Supply

i. Switch shall be configured with Redundant hot-swappable internal power supplies

ii. Switch shall be configured with Hot-swappable fan assembly

iii. Power Supply: Should be offered with two internal, redundant, field- replaceable, hot-swappable AC power supplies (100 to 240 VAC, 50 to 60 Hz)

iv. All the switches shall be delivered with required power cables with C13 PDU cables with suitable length (3 Ft or 5 Ft).

l. Switch Management

i. Command-line interface

ii. Out-of-band management (RJ-45 Ethernet and serial RS-232C/Micro USB)

iii. SNMP Manager

iv. Console cable to be included with each switch

v. The proposed switch should have enough Memory (Flash and RAM) to hold the latest Software Release. Switch should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc.

vi. Switch should support for execution of script for device management for automatic and scheduled system status update for monitoring and management

m. Reliability

i. Switch shall have MTBF 150,000 Hours or better. Vendor shall provide required datasheet or OEM certification to establish MTBF of the offered hardware.

ii. Components, like modules/ power supplies/ fan tray should be Hot Swappable. Online insertion and removal (OIR) support is must for modules, Power supply and FAN.

iii. Switch should support for (Bidirectional Forwarding Detection) BFD for Multipoint network for fast Failure Detection as per RFC 5881 or equivalent

n. **Environmental regulatory compliance.** Following or equivalent international certifications

i. RoHS India [E-Waste (Management) Rules, 2016] certification

Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

ii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer/ Hardware

iii. Security Compliance – OEM signed image verification

iv. Valid Indian Common Criteria Certification Scheme (IC3S) for EAL2 or better for the offer product or offered version of firmware

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

6. Appendix 'F' – Core Switch

Specifications for Core Switch

a. **Physical.** 19-inch rack mountable chassis along with rack mount kit.

b. Chassis.

i. Switch should not be configured with any over-subscribed line interface cards.

ii. The configuration for an individual switch shall be realized using a single chassis.

iii. The offered chassis should not have any active components in unloaded condition (bare chassis without any line cards and power supplies)

c. Fabric

i. The Switch should provide a non-blocking, distributed switching fabric architecture

ii. Management functionality should be available with full redundancy

iii. In case, the management functionality is integrated with a line card, then redundancy shall be provided by duplicating that card or by an alternate card supporting management functionality

iv. Failure of any supervisor engine or fabric module should not bring down the performance, redundant components needs to be proposed accordingly.

v. Switch fabric to be provided with redundant switch fabric capability

vi. The architecture of the switching fabric should be modular & Hot Pluggable

d. Port Requirement – Each Switch shall be configured with

i. 1/10 G Ethernet Port = 96 Nos, Can be offered with 40 Nos 1G Copper and 56 Nos 10G Coper interface native or with Transceiver with suitable line card arrangement if 1/10G native Copper Interface line cards are not available

ii. 1/10/25 G Fiber - 48 No

iii. 40/100 Gbps QSFP uplink ports (SR/LR) = 4 Nos. 40/100G ports Shall be offered through two or more independent line cards

iv. Each switch shall have following transceivers loaded

1) 1G (SX) SFP LC = 10 Nos

2) 1G (LX) SFP LC (Upto 10 KM)= 8 Nos

3) 10G (LR)SFP+ LC (Upto 10 KM) = 8 Nos
4) 10G (SR)SFP+ LC = 8 Nos
5) 25G (SR) SFP28 LC = 4 Nos
6) 40G (SR) BiDi QSFP+ LC = 4 Nos

v. The transceivers offered should be from the same switch manufacturer (OEM) only

e. Performance-

i. Per slot minimum 6.0 Tbps bandwidth.

ii. Latency - The Switch should have capability to support latency as low as 3.98 microsec for packet size of 64-Bytes.

iii. The offer chassis shall be capable to support 100G ports 30 Nos in single line card in non-blocking mode in all payload slot of the chassis

iv. The Switch should have a Truly Distributed Architecture. All Interface Modules should have all the resources for switching and Routing and should offer True Local Switching (Intra-Module and Inter-Module).

v. Switch should support minimum 128 VRF instances with route leaking functionality

vi. The Switch should support 350k IPv4 LPM routes

vii. The line card proposed in the Switch should have minimum 32MB packet buffer and it should support minimum of 64MB of buffer on 100 Gig line Cards.

viii. The Switch should support 100k multicast routes

ix. Switch platform should support MAC Sec (802.1AE) in hardware for 100G ports.

f. **SDN Feature.** The offered switches shall be hardware ready for SDN support.

g. Layer 2 Features –

i. VLAN support and tagging (IEEE 802.1q)

ii. Spanning Tree Protocol (IEEE 802.1D, 802.1W,802.1S)

iii. MAC Address Locking and MAC layer Filtering

iv. MAC Address Locking and MAC layer Filtering

v. IGMP v2

vi. PIM-SM Snooping, Support Multicast Source Discovery Protocol (MSDP) - RFC 3618

vii. Jumbo packet support, Max Size=9000 Bytes

viii. Rapid Per-VLAN Spanning Tree (RPVST+)/ RSTP or equivalent

h. Layer -3 Features –

i. VRF/ VRF Lite
ii. VRF Leaking
iii. BGP RFC 4271
iv. OSPF and IS-IS
v. VRRP/ VRRP-E / HSRP
vi. RIP v2
vii. Multicast Routing RFC 2858 or equivalent
viii. Generic Routing Encapsulation (GRE)

i. IPV6 Support –

i. IPv6 Routing (OSPF v3), BGP4+ (IPv6)
ii. OSPF for IPv6
iii. VRRP-E (IPv6)/ HSRP(IPv6)/VRRPv3
iv. VRF (IPv6)
v. IPv6 over IPv4 tunnels
vi. Multicast Listener Discovery (MLD) version 2 snooping

j. Security Features –

i. MAC Authentication
ii. Protection against Denial of Service (DoS) attacks
iii. Encryption -- Must support 128-bit Advanced Encryption Standard (AES) for SSL/Management encrypted traffic
iv. ACL - Provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number
v. Must support switch-port configuration to block flooding of unknown multicast or unicast traffic.
vi. Must support traffic storm control to monitor the levels of the incoming broadcast, multicast, and unicast traffic against a set threshold and filter out subsequent packets when a threshold is reached.
vii. TPM 2.0 or Secure boot or should support image verification with OEM signed certificates

viii. Time based ACL or Equivalent

k. Supported Protocol and RFC Standards-

i. 802.1D Bridging

ii. 802.1q VLAN Tagging

iii. 802.1p Mapping to Priority Queue

iv. 802.1w Rapid Spanning Tree (RSTP)

v. 802.3ad Link Aggregation

vi. 802.3x Flow Control / Priority-based flow control (PFC) - 802.1Qbb

vii. SNMP V1, V2, V3

viii. RFC 950 Internet Standard Subnetting Procedure

ix. RFC 1403 BGP OSPF Interaction or should support route exchange between protocols

x. RFC 4632 Classless Inter-Domain Routing (CIDR)

xi. RFC 4604 Internet Group Management Protocol (IGMP) Version 3

xii. RFC 4291 IPv6 Addressing Architecture

xiii. RFC 1981 Path MTU Discovery for IPv6

xiv. RFC 4193 / RFC3587 Unique Local IPv6 Unicast Addresses

xv. RFC 6241 Network Configuration Protocol (NETCONF)

xvi. RFC 4861 or equivalent for Neighbor Discovery for IP Version 6 (IPv6)

xvii. RFC 3623 Graceful OSPF Restart

xviii. RFC 5308 Routing IPv6 with IS-IS

xix. RFC 1195 Use of IS-IS for Routing in TCP/IP and dual environment

xx. OEM can refer to updated or equivalent RFC wherever applicable

l. Virtualization Features (VPC or VCS)

i. VXLAN (RFC 7348)

ii. VX LAN Routing, VXLAN Bridging , VRF aware VXLAN Routing / Multi tenancy

iii. Switch should support layer 2 extension over VXLAN (RFC7348) across all DataCenter to enable VM mobility & availability

iv. Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890

m. Reliability and Availability

i. The Switches should have hardware level redundancy in terms of data plane and control plane. Issues with any of the plane should not impact the functioning of the switch

ii. Chassis shall have MTBF 450,000 Hours or better. Vendor shall provide required datasheet, certification or a signed legal letter to establish MTBF of the offered chassis.

iii. There should not be any single point of failure in the switch. All the main components like CPU module, switching fabric, support module, system clock, power supplies and fans etc should be in redundant configuration.

iv. Components, like modules/ power supplies/ fan tray should be Hot Swappable. Online insertion and removal (OIR) support is must for modules, Power supply and FAN.

v. Module replacement should not require rebooting of the switch or create disruption in the working of the switch.

vi. Switch should support for (Bidirectional Forwarding Detection) BFD for Multipoint network for fast Failure Detection as per RFC 5881 or equivalent RFC

vii. The chassis should Support Dual Supervisor based In service Software Upgrade (IISU)/ Graceful Routing Engine Switchover (GRES) with NonStopForwarding/equivalent

viii. There should not be any impact on the performance in the event of the software upgrade/downgrade.

n. Power Supply –

i. The switch should be offered with hot swappable redundant Power Supply Units with N+N configuration

ii. The offered power supply must meet 80 Plus Silver or better power efficiency. For make in India products as per Bureau of Energy Efficiency, Govt of India Guideline for Computer the compliance shall be submitted.

iii. The offered power supply units should be able to drive the switch in fully loaded configuration with full redundancy

iv. The power supplies shall be rated for 230 V, 50 Hz operation.

v. Matching type of power cables shall be offered with each switch to connect to panel

o. Cooling

i. The switch should be offered with hot swappable redundant cooling fans loaded in each chassis

ii. The blowing of air shall be front to rear flow. Side blowing configuration shall not be accepted.

iii. The cooling fans shall be loaded to the full capacity of the chassis

p. Switch Management –

i. Device can be managed by command-line interface by SSH; out-of-band management (RJ-45 Ethernet); SNMP Manager; Telnet and FTP; out-of- band management (serial RS-232C or Micro USB)

ii. In case, the management functionality is integrated with a line card, then redundancy shall be provided by duplicating that card or by an alternate card supporting management functionality

iii. Management function shall be state synchronized in active-active or active- standby mode through redundant supervisory cards.

iv. The proposed switch should have enough Memory (Flash and RAM) to hold the latest Software Release. Switch should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc.

v. Switch should support for execution of script for device management for automatic and scheduled system status update for monitoring and management

q. **Environmental regulatory compliance and Certification.** The offered switch must have following certification or equivalent international certification:

i. RoHS India [E-Waste (Management) Rules, 2016] certification Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

ii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer/ Hardware

iii. Security Compliance – TPM 2.0 or Secure boot or should support image verification with OEM signed certificates

iv. Valid Indian Common Criteria Certification Scheme (IC3S) for EAL2 or better for the offer product or offered version of firmware

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

7. Appendix 'G' – Network Security Appliance

1. Specifications for Network Security Appliance:

The Network Security Appliance required for the operational Network to include the following devices under single OEM make. Bidder may note that the reference to a specific OEM hardware model is only to define capability and sizing of the product and not to restrict brand. Bidder may offer any OEM product which has same technical capability as mentioned in the RFP. Following devices are required:

No	Device
a.	UTM/Next Generation Firewall (NGFW) – Config 1 & 2
b.	Next Generation Firewall (NGFW) Logger & Traffic Analyser
c.	Next Generation Firewall (NGFW) Manager
d.	UTM Hardware Authentication Token
e.	End Point Protection & Management Capability

a. UTM/Next Generation Firewall (NGFW) - Config-1

i. **Specification**- Next generation Firewall with integrated IPS, IDS, Antivirus and Gateway-antivirus, as per detailed specifications below. Vendor can quote products equivalent or better to Fortigate 121G (Part No. FG-121G) with Unified Threat protection.

ii. Physical and General Specification –

1) 19-inch rack mountable chassis along with rack mount kit. Offered device shall be with-in 2U form factor.
2) The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened proprietary operating system. The firewall appliance should support Integrated IPS, IDS, DLP, DoS, Web-Filtering, Antivirus and Application control feature.
3) The firewall appliance should support dual stack IPv4 and IPv6
4) The proposed solution should support dynamic routing like RIP1, RIP2, OSPF, BGP4.
5) Device shall support for upto 10 nos of firewall virtual partitioning. Each partition/instance should act as independent firewall with all features and should have independent users and resource management capabilities.
6) The UTM/NGFW shall have provision for integration with centralized management and definition update by specialized firewall manager device. The centralized manager will be form the same OEM of offered UTM/NGFW make.
7) The UTM/NGFW shall have centralized logging and report generation device by same OEM make as a specialized hardware for traffic report generation.

iii. Port Requirement –

1) The UTM/NGFW shall be offered with 1G RJ45=16 Nos, 1G Fiber=8 Nos, 10G Fiber=4 Nos with 02 Nos of 10GE SFP+ and 08 Nos 1G single mode LC SFP transceivers (Upto 2 KM),

2) The transceivers offered should be from the same OEM or OEM Certified.

iv. General Features –

1) The NGFW shall have Storage: 480 GB SSD internal storage.
2) Firmware should reside on Internal Flash.
3) The internal SSD and Firmware Flash shall be removed and retained with User during a device replacement or during any failure in SSD or Flash.
4) The proposed solution should have unrestricted user/node license.
5) The proposed solution must support user based policy configuration for security & management.
6) The proposed solution should support Route (Layer 3), transparent mode (Layer 2) and MIX mode deployment.

v. Performance –

1) The offered NGFW shall have following performance figures for Enterprise traffic mix - Firewall: 28 Gbps (with 64 Byte UDP Packet), IPS: 5.3 Gbps, NGFW:3.1 Gbps, Threat Protection Throughput 2.8 Gbps, Firewall Latency: 3.17 microsecond (for 64 Byes UDP packet) or better
2) Device shall support minimum 2000 Nos of IPSec Site-to-Site VPN
3) The configuration for an individual Firewall shall be realized using a single chassis (not by stacking).

vi. Administration, Authentication & General Configuration Feature –

1) The proposed solution should support administration via secured communication over HTTPS, SSH and from Console.
2) The proposed solution should be able to export and import configuration backup including user objects.
3) The proposed solution should support user/ip/mac binding functionality to map username with IP address & MAC address for security reason.

vii. IPV6 Support –

1) IPv6 Routing
2) IPv6 Multicast Routing
3) IPv6 over IPv4 tunnels

viii. High Availability Features –

1) The proposed solution should support High Availability Active/Passive or Active/Active deployment. The license shall be offered along with the product
2) The proposed solution should support Link, device & Session failure.
3) The proposed solution should support automatic & manual synchronization between appliances in cluster

ix. Power Supply –

1) Should be offered with internal, redundant power supplies (220 VAC at 50 Hz)
2) Required number of power cables (IEC-13/14 Power Cord 2 Meter) shall be offered with each device

x. Firewall Management command-line interface; Web browser; out-of-band management (RJ-45 Ethernet); SNMP Manage; out-of-band management (serial RS-232C or Micro USB)

xi. Environmental regulatory compliance

1) RoHS-compliant / RoHS India
2) FCC and CE norm or equivalent as per Govt. of India guideline

xii. **Product Certification Security Certification -** Valid Indian Common Criteria Certification Scheme (IC3S) for EAL4 or equivalent certification for the offered device or firmware.

b. UTM/ Next Generation Firewall (NGFW) - Config-2

i. **Specification-** Next generation Firewall with integrated IPS, IDS, Antivirus and Gateway-antivirus, as per detailed specifications below. Vendor can quote products equivalent or better to Fortigate 91G(Part No. FG-91G) with Unified Threat protection.

ii. Physical and General Specification

1) 19 inch rack mountable chassis along with rack mount kit. Offered device shall be with-in 2U form factor.
2) The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened proprietary operating system. The firewall appliance should support Integrated IPS, IDS, DLP, DoS, Web-Filtering, Antivirus and Application control feature.
3) The firewall appliance should support dual stack IPv4 and IPv6
4) The proposed solution should support dynamic routing like RIP1, RIP2, OSPF, BGP4.
5) Device shall support for upto 10 nos of firewall virtual partitioning. Each partition/instance should act as independent firewall with all features and should have independent users and resource management capabilities.
6) The UTM/NGFW shall have provision for integration with centralized management and definition update by specialized firewall manager device. The centralized manager will be form the same OEM of offered UTM/NGFW make.
7) The UTM/NGFW shall have centralized logging and report generation device by same OEM make as a specialized hardware for traffic report generation.

iii. Port Requirement

1) The UTM/NGFW shall be offered with 1G RJ45=8 Nos, , 1G/10G Fiber= Nos with 02 Nos of 1G single mode LC SFP transceivers (Upto 2 KM).
2) The transceivers offered should be from the same OEM or OEM Certified.

iv. General Features

1) The NGFW shall have Storage: 120 GB SSD internal storage.
2) Firmware should reside on Internal Flash.
3) The internal SSD and Firmware Flash shall be removed and retained with User during a device replacement or during any failure in SSD or Flash.
4) The proposed solution should have unrestricted user/node license.
5) The proposed solution must support user based policy configuration for security & management.
6) The proposed solution should support Route (Layer 3), transparent mode (Layer 2) and MIX mode deployment.

v. Performance

1) The offered NGFW shall have following performance figures for Enterprise traffic mix - Firewall: 27 Gbps (with 64 Byte UDP Packet), IPS: 4.5 Gbps, NGFW:2.5 Gbps, Threat Protection Throughput 2.2 Gbps, Firewall Latency: 3.23 microsecond (for 64 Byes UDP packet) or better
2) Device shall support minimum 2000 Nos of IPSec Site-to-Site VPN

3) The configuration for an individual Firewall shall be realized using a single chassis (not by stacking).

vi. Administration, Authentication & General Configuration Feature

1) The proposed solution should support administration via secured communication over HTTPS, SSH and from Console.
2) The proposed solution should be able to export and import configuration backup including user objects.
3) The proposed solution should support user/ip/mac binding functionality to map username with IP address & MAC address for security reason.

vii. IPV6 Support –

1) IPv6 Routing
2) IPv6 Multicast Routing
3) IPv6 over IPv4 tunnels

viii. High Availability Features –

1) The proposed solution should support High Availability Active/Passive or Active/Active deployment. The license shall be offered along with the product
2) The proposed solution should support Link, device & Session failure.
3) The proposed solution should support automatic & manual synchronization between appliances in cluster.

ix. Power Supply

1) Should be offered with redundant power supplies (220 VAC at 50 Hz)
2) Required number of power cables (IEC-13/14 Power Cord 2 Meter) shall be offered with each device

x. Firewall Management command-line interface; Web browser; out-of-band management (RJ-45 Ethernet); SNMP Manage; out-of-band management (serial RS-232C or Micro USB)

xi. Environmental regulatory compliance –

1) RoHS-compliant / RoHS India
2) FCC and CE norm or equivalent as per Govt. of India guideline

xii. **Product Certification Security Certification -** Valid Indian Common Criteria Certification Scheme (IC3S) for EAL4 or equivalent certification for the offered device or firmware.

c. Next Generation Firewall (NGFW) Logger and Traffic Analyzer

i. **Specification-** Vendor can quote products equivalent or better to Fortigate FAZ- 1000G (Part No.FAZ-1000G). The NGFW logger and Traffic Analyzer shall be a same OEM make specialized device or appliance as the offered NGFW.

ii. Physical and General Specification –

1) The firewall logger device shall be a dedicated appliance based device with 24TB Storage capacity (with RAID protection) for logging the firewall logs, 4 x 1GbE RJ45 Network Interface, 2x 1GbE SFP Interface, and up to 660 GB/Day of Logs.
2) The logger shall have capability to partition the Logger to have dedicated Logging instance

from different network segments with-out mixing traffic from other segment.

3) The failed disks shall not be returned back during warranty support.
4) The logger shall have advance analytics capacity and shall also work as a SOC for UTM traffic
5) The device shall show traffic log, event log, DNS log, security logs etc in different category
6) The device shall support custom and automated report generation and shall integrate with Email
7) Device shall have hot swappable redundant power supply.
8) Device shall support TPM 2.0

d. Next Generation Firewall (NGFW) Manager

i. **Specification-** Vendor can quote products equivalent to Fortigate FMG- 200G(Part No. FMG-200G). . The NGFW Manager shall be a same OEM make specialized device or appliance as the offered NGFW.

ii. Physical and General Specification –

1) The firewall manager device shall be a dedicated appliance based device.
2) The product shall support 30 Devices/UTM partitions
3) Device shall be 1 U Rack Mount
4) Device shall have 4 Nos of 1G interfaces
5) Device shall support TPM 2.0
6) Storage Capacity 4TB with RAID protection
7) Device shall have hot swappable redundant power supply configured.

e. Hardware Authentication Token

i. **Specification-** Vendor can quote products equivalent to Fortitoken 210. The Token shall be a same OEM make specialized device or appliance as the offered NGFW.

ii. Physical and General Specification –

1) The physical token shall be TOTP complaint
2) The device shall be tamper resistant/ tamper evident package.
3) Device shall have minimum 3 years life time.
4) The device shall have Lithium non chargeable internal battery.
5) Device shall be Water Resistance IP-65 certified.
6) Device shall be delivered with suitable key seeding option so that keys can be migrated from failed hardware to new hardware. If such feature is not offered, during every RMA OEM to provide key seeding feature.

f. End Point Protection & Management Capability

i. **Specification-** Vendor can quote products equivalent to Fortigate Central Management Tool Endpoint Management System (EMS) and Forticlient End Point Protection and ATP Services with managed services. All the elements shall be deliverable from the same NGFW make and integrated in a single fabric.

ii. Physical and General Specification –

1) The Central Management Tool Endpoint Management System shall be a KVM deployable VM.
2) The offered end point protection product shall be enterprise class software with device control, application control and anti-malware feature.
3) The end point control software shall be certified for windows and Linux platform.
4) The solution shall provide security fabric integration with manager and logger device
5) The solution shall provide compliance and ATP for client nodes
6) The EMS license shall provide Provisioning, Compliance and Security Fabric, Remote Control, Telemetry and Monitoring feature for the end points.

g. **POC Requirement for NGFW UTM and associated Components** During evaluation process NSIL may need to conduct POC for the offered NGFW and associated products (Manager, analyzer, Client and compliance node) to evaluate the offered product capability. NSIL purchase shall intimate vendor to arrange for required infrastructure on physical or VM infrastructure to carry out feature evaluation of the products and verification of the integration of the components. Vendor has to offered the required infrastructure within two weeks after receipt of the POC requirement. NSIL will need remote access to the infrastructure for carrying out the evaluation.

h. **Hardware Upgrade:** For Item supplied as part of Network Security Appliance, during the support period offered, the offered hardware does not support OEM supported firmware due to hardware obsolesces, vendor needs to provision supported hardware of equivalent configuration and migrate the services in new platform.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

8. Appendix 'H' – Interconnection Router

a. Specification for Interconnection Router Config- 1 as follows for per router -

i. C8300-1N1S-6T Cisco Catalyst C8300-1N1S-6T Router - 1 No

ii. CON-SNT-C830IN6T SNTC-8X5XNBD Cisco Catalyst C8300 - As per support duration

iii. MEM-C8300-8GB Cisco Catalyst 8300 Edge 8GB memory - 1 No

iv. M2USB-16G Cisco Catalyst 8000 Edge M.2 USB 16GB - 1 No

v. C-RFID-1R Cisco Catalyst 8000 Edge RFID - 1RU - 1 No

vi. C8300-RM-19-1R Cisco Catalyst 8300 Rack mount kit - 19" 1R - 1 No

vii. C8300-PIM-BLANK Cisco Catalyst 8300 Edge PIM Blank - 1 No

viii. NETWORK-PNP-LIC Network Plug-n-Play Connect for zero-touch device deployment - 1 No

ix. IOSXE-AUTO-MODE IOS XE Autonomous boot up mode for Unified image - 1 No

x. SC8KBEUK9-173 UNIVERSAL - 1 No

xi. PWR-CC1-400WAC Cisco C8300 1RU AC Power supply - 2 Nos

xii. CAB-IND AC Power Cord (India) - 2 Nos

xiii. NIM-ES2-4 4-port Layer 2 GE Switch Network Interface Module - 2 No

xiv. C-SM-NIM-ADPT Cisco Catalyst SM to NIM Module Adaptor - 2 No

xv. GLC-LH-SMD= 1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM - 2 Nos

xvi. Console Cable – 1 No

P1: The routers must include the Cisco DNA advantage license with full L3 capability. The part numbers listed above is for providing the description of the capability required.

P2: Vendor may note that the part number of Cisco is subject to change. These part numbers are mentioned as indicative. Vendor needs to select the latest part number and equivalent or better feature and offer the complete BOM.

1. **P3.** Vendor may also offer router of different make/OEM but with all equivalent physical characteristics and logical features. In such case, vendor may provide a mapping document to show how the features are offered in different make.

b. Specification for Interconnection Router Config- 2 as follows for per router -

i. C1121X-8P ISR 1100 8P Dual GE SFP WAN 8GB Router- 1 No

ii. CON-SNT-C1121X8P SNTC-8X5XNBD ISR 1100 8P Dual GE SFP WAN 8GB Router- (As per support duration)

iii. PWR-66W-AC-V2 - Power Supply 66 Watt AC V2 for C890 and C1100 series – 1 No

iv. SL-1K-8P-IPB IP Base License for Cisco ISR 1120 and 1160 8 Ports Series – 1 No

v. CAB-IND - AC Power Cord (India) – 1 No

vi. ACS-1100-RM2-19- Cisco 1100 Series Router Rackmount Kit – 1 No

vii. SISR1100UK9-176 Cisco ISR1100 Series IOS XE – UNIVERSAL – 1 No

viii. L-DNA-TIER-ADD Cisco DNA Subscription License for Routing and SD-WAN – 1 No

ix. C1100-8P-DNA-PF - ISR1100 8-Port Platform Selection for DNA – 1 No

x. IOSXE-AUTO-MODE-PF IOS XE Autonomous or SD-Routing mode for Unified image – 1 No

xi. DNA-P-T0-A-5Y - Cisco DNA Advantage On-Prem Lic 5Y - upto 25M (Aggr, 50M) – 1 No

xii. SL-1100-8P-NA-A-L Cisco ISR1100 8 Port Network Stack Advantage Lic – 1No

xiii. Console Cable – 1 No

P1: The routers must include the Cisco DNA advantage license with full L3 capability. The part numbers listed above is for providing the description of the capability required.

P2: Vendor may note that the part number of Cisco is subject to change. These part numbers are mentioned as indicative. Vendor needs to select the latest part number and equivalent feature and offer the complete BOM.

2. **P3.** Vendor may also offer router of different make/OEM but with all equivalent physical characteristics and logical features. In such case, vendor may provide a mapping document to show how the features are offered in different make.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

9. Appendix 'I' – Server Room Structured Cabling and Accessories

a. LAN Cables & Accessories and Structured Cabling

Quantity – The Following LAN cables needs to be delivered. The make of the LAN cable shall be Legrand, Molex, CommScope, AMP, 3C3 or equivalent quality:

No.	Item Description	(Nos.)
1.	1G Ethernet 3 Meter (Color - Green)	200
2.	1G Ethernet 3 Meter (Color - Yellow)	200
3	1G Ethernet 5 Meter (Color - Gray)	150
4.	1G Ethernet 10 Meter (Color - Red)	50
5.	1G Ethernet 15 Meter (Color - Blue)	40
6.	10G Ethernet 3 Meter (Color - Blue)	100
7	10G Ethernet 5 Meter (Color - Reg)	50

General Specification - The offered CAT6 cables should comply the following Standards/certifications:

i. Performance Characteristics – As per ISO/IEC 11801 2nd Edition or better

ii. Fire/Flame Rating – As per IEC 60332-1 or better

b. Power Cables (Brands --- Legrand, ABB or equivalent quality)

i. Cable Type-1: Industrial Standard Power Cord with IEC-13 and IEC-14 Connector on either side, 2M/6inch =250 Nos.

ii. Cable Type-2: Industrial Standard Power Cord with IEC-19 and IEC-20 Connector on either side, 2M/6inch=50 Nos.

1. NOTE: Any additional power/LAN cables required to connect components that are in the scope of this tender to be provided by the vendor at no additional cost.

c. Rack to Rack Structured Cabling for 10G Ethernet

i. There are six server Racks and six network racks which are placed facing to each other with a gap as shown in diagram. They are positioned in user server room. Each server Rack has to be provisioned with two CAT6A 24 port fully loaded patch panel. These patch panels needs to be mounted on the rear end of the rack. Thus total of 12 nos

of CAT6A 24 port fully loaded

patch panel will be installed for 10G I/O ports (considering six server racks). Each patch panel on server rack side shall have other end terminated on the central network Rack (Network Rack 3 and Network Rack 4) respectively as shown in diagram. Structured Cabling work is required at Bhopal for 10G I/O ports.

ii. Similarly, there will be requirement for 24 Port patch panel (Cat -6A) – between Network Rack 1 to Network Rack 3 and Network Rack 4 to Network Rack 6.

iii. The following table shows the total cable requirement for patch panels.

Description	Reqd. cable length (mt)	Ports/ patch panel	No.of patch panels	No of CAT -6A IO	No of data point for termination	No.of Racks	Total Cable Length (mt)
Server rack to Network rack	10	24	2	576	288	6	2880
Network rack to Network Rack	5	24	2	96	48	---	240
*Aggregated 4-pair CAT6A UTP cable required for patch panels							3120

iii. Vendor must note that there may be 10% variation in estimation. Vendor must include the cost considering the variation in cable length and make the commercial offer.

iv. Vendor shall use Legrand, Molex, CommScope, AMP, 3C3 or equivalent quality

v. Vendor shall install the data points and certify the Cat6A LAN certifier device. The following is the scope of data point installation

1) Data Points mentioned in the RFP mean end-to end point installation
2) Laying of 4-pair, Cat 6A UTP Cable through PVC conduit Pipes/Casing. Required conduit pipe and casing must be included in the offer
3) Fixing and Termination of Information outlets and patch panel
4) Labeling of the patch panels, UTP cables for proper tractability and mapping of the ports
5) Dressing of Cables, with Proper end-to-end labelling of cables with ferules and each data-point.
6) Documentation and Testing of Data Points Using measuring test Instruments. Vendor has to arrange suitable cable certified (LAN certifier device) for CAT-6A for certification. Vendor must produce valid calibration certificate of the LAN tester before using it at site.

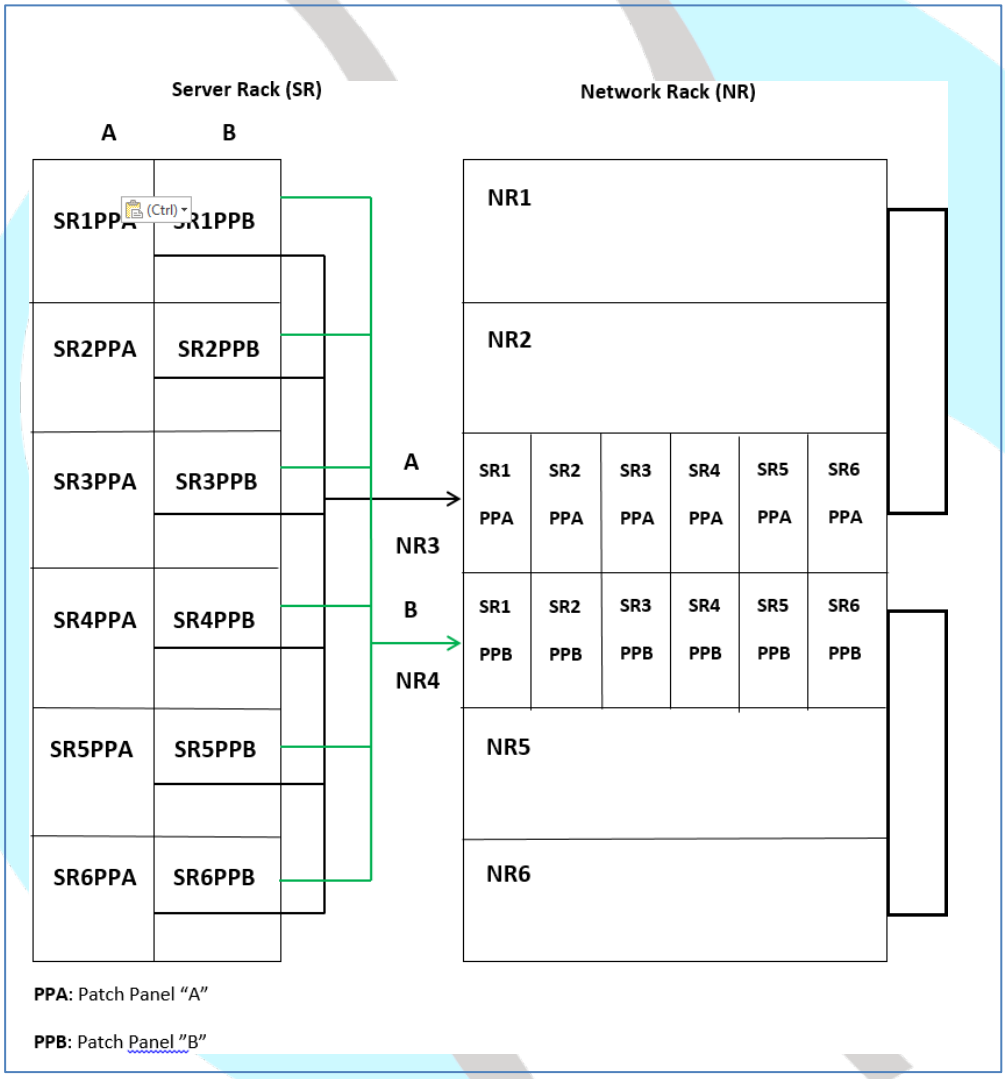


Figure: Shows the connectivity how racks needs to be provisioned with 10G structured cabling

10. Appendix 'J' – All in One PCs

a. System Specifications -

i. Pre-installed with Windows 11 Professional or latest version of windows

ii. Slots: Two DIMM, loaded with 16 GB memory configured

iii. Processor: Latest Generation Intel/AMD Processor with 14 cores, 2.5 GHz and 24 MB cache or higher processor.

iv. Hard Disk Drive: 1 TB SSD

v. Ports: USB Version 3.0 / 3.1, Ports: 4; USB Type C Ports: 1; VGA Ports: 1; HDMI Ports: 1; DP Port: 1; RJ-45 Ethernet Port – 1 No

vi. USB Multimedia keyboard and optical mouse

vii. POWER: 100-240V AC

viii. Required power adapter or Cable to be provided.

ix. The offered system will be all-in-one PC system and not a Personal Computer with independent Monitor, CPU, Speaker Webcam and Microphone. Vendors who offers solution on general purpose PC, will be rejected.

x. The hardware offered shall not have any in-built wifi interface and in-built Bluetooth interface. The system offered shall not have these features built on the chipset. If any vendor offer systems which has in-built wifi interface and in-built Bluetooth interface and is disabled through BIOS software, such systems shall not be accepted for evaluation. Vendor may note that, this is a security requirement and the compliance is must.

xi. System shall be delivered with OEM make 100mm VESA mount for mounting on work-console arms.

b. Display Screen Specifications and features

i. Display Size (INCHES): 23.8 or better

ii. Display Type: Non Touch

iii. Panel Technology: IPS

iv. Display Resolution (PIXELS): 1920x1080 or better

v. Availability of Webcam integrated with Display: NO

vi. Availability of Webcam integrated with Display: NO

vii. Availability of Speakers integrated with Display: Yes (two numbers)

c. Certification

i. RoHS, BIS, BEE or equivalent international certification

ii. TPM

iii. Windows 11 certified

d. Software to be included along with media with each PC -

i. Windows 11 Professional

ii. Microsoft Office Professional latest version

iii. Pre-loaded antivirus software with support for 5 years

e. Bluetooth and WiFi: Should NOT BE integrated with the system. WEBCAM should not be present.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

11. Appendix 'K'– NMS Rugged Laptops

a. Network Management System (Rugged Laptop)

i. 14 inch fully rugged laptop

ii. Serial to USB Adapter – 2 Nos with each laptop

b. Specification

i. Pre-installed with Windows 11 Pro

ii. Intel core i-5 or AMD Processor

iii. 16 GB DDR4 RAM .

iv. 512 GB NVMe OPAL SSD

v. Ports: 2x USB 3.2, 1 HDMI out display port, 1 LAN

vi. Inbuilt microphone, camera and speaker

vii. Battery life upto 36 Hours (if required additional battery to be loaded in the configuration)

viii. 14 inch Full-HD Touch Active Matrix LCD, 1.200 d/m2

ix. DVD Multi Drive =1

x. Security – TPM 2.0

xi. Required power adapter and cable to be provided.

xii. IP66 Ingress protection

xiii. IP65 Dust Resistant

xiv. Drop Resistance = 180 cm

xv. Operating Temperature = -29 to + 63 degree celcius

c. Software to be bundled along with each Laptop

i. Windows 11 Professional

ii. Microsoft Office Professional latest version

iii. Antivirus software with 5 years subscription

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

12. Appendix 'L' – Automatic Transfer Switch (ATS)

Specification – ATS shall have following or better specification:-

a. Input

i. Input Connections =2 Nos.

ii. Nominal Input Voltage should be 220-240V

iii. Input Frequency = 47-63 Hz

iv. Input Connections should be IEC-320 C20

v. Maximum Line Current per phase =20A

vi. Maximum Input Current per phase =20A

b. Output

i. Output Connections=9

ii. Nominal Output Voltage = 220-240V

iii. Maximum Total Current Draw per Phase=16A

iv. Output Connections type IEC-320 C13=8

v. Output Connections type IEC-320 C19=1

vi. Overload Protection=No

c. **Physical:** 19 inch Rack mountable unit with rack mount kit. Rack Mounting Bracket or Mounting Rails should be included with the base product

d. Front Panel

i. Input Source Selection using push button with-out disturbing output should be possible

ii. Selected Source Should be visible on the front Panel

iii. Digital Display for current drawn per power Distribution

iv. Display should warn when current drawn is close to the maximum draw of the strip.

e. Remote Management Capability –

i. Offered product should be managed via Web ,SNMP , and Telnet

ii. Allows users to access , Configure , and manage units from remote locations

iii. Firmware should be upgradable via network

f. **High Availability:** Two AC Lines should power the Unit and if the primary AC power fails, the unit should automatically switch to the alternate power source within 20ms or without circuit breaker.

g. **Cooling:** Sufficient cooling shall be provisions

h. **Power Cord:** All Cables Should be RoHS Compliant. Power Cable shall be only from a proven product line from highly reputed manufacturers.

i. Regulatory Compliance

i. Operating Environment: -5 to 45 degree C
ii. Operating Relative Humidity: 5 to 95 %
iii. Storage Temperature: -25 to 65 degree C
iv. Storage Relative Humidity: 5 to 95 %

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

13. Appendix 'M' – Station Computers and AIO Thin Clients

Station Computer Server (STC) Server Specification

a. Processor –

i. Make & Architecture Intel CISC(X86-64),

ii. 8 Cores (16 threads) per processor or better,

iii. Processor Base frequency 2.6GHz,

iv. Processor Turbo Frequency 4.1 GHz,

v. Processor Description/ Number Intel Xeon Silver 4509Y or better or equivalent

b. **Chassis -** Form factor Rack, Size 1 RU

c. Motherboard -

i. Chipset compatible with CPU Intel C741 or better

ii. Expansion Slots Gen 3 (PCIe x16)- 1 or more

iii. Minimum number of Sockets populated with Processors on Server – 2 or more

d. Memory –

i. Type of RAM: DDR4 SDRAM with ECC or better

ii. Total Number of DIMM Slots: 32

iii. Minimum Number of DIMM Slots populated with DDR SDRAM: 2

iv. DDR SDRAM Size(GB): 128 or more

v. DDR SDRAM upgradable upto using spare DIMM Slots (GB): 960 or more

e. SSD Storage –

i. Type of Interface for SSD: SAS

ii. Type of SAS SSD: Mixed Use

iii. SAS SSD Hot Swappable: Yes

iv. Endurance for SAS SSD (DWPD - Drive Writes Per Day) (X): 1 or better

v. Total Number of Slots for SAS SSD: 8 or better

vi. Number of Slots shall populate with SAS SSD: 2 or more

vii. Minimum Capacity SAS SSD (GB) or more: 960 or better

viii. Total Capacity SAS SSD (GB) or more: 1920 or better

f. RAID –

i. RAID level: 1

ii. No of RAID Controller Ports: 8

iii. Speed of RAID Controller Ports (Gbps): 12

g. Ports & Interfaces

i. Network Card: 1G

ii. Number of Networking Interface Cards (LAN): 3

iii. Whether Network Interface Card Embedded: No

iv. Total Number of 1G Ethernet Ports required in Server: 10 X 1G

v. DVD-RW (Internal/External): Yes

vi. USB Ports (3.0) Minimum: 3

vii. Total number of Spare Bays for Future Upgradation (Hot Pluggable): 8 or more

h. Certifications –

i. Certifications/Compliance (OS) - Windows server 2022 standard edition or latest, Red Hat Enterprise Linux 9.2 or latest. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

ii. Compliance & Certifications – Following or equivalent international certification

- RoHS India [E-Waste (Management) Rules, 2016] certification
- Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard
- Security Compliance – TPM 2.0, UEFI Secure boot

i. **Operating System –** Redhat Enterprise Linux Server latest edition

j. Management features

i. IPMI 2.0 compatible management capability with dedicated management LAN

k. Generic

i. Redundant Power Supply - Yes

ii. Hot Swappable (Redundant Power Supply) - Yes

iii. Power Supply Efficiency - Platinum

iv. Redundant Fan - Yes

v. Hot Swappable (Redundant Fan) - Yes

vi. Server Main Supply - 230 +/- 10%Vac

I. All in one thin client (AIO) for Display & Remote access with Specifications as below:

i. Processor - 2.5 GHz or above.

ii. System memory- 8 GB DDR4 or above/better.

iii. Flash memory - 256 GB PCIe NVMe SSD or above.

iv. Display - 24 inch or above.

v. Display resolution - 1920 x 1080 FHD at 60 Hz, anti-glare or better and Color support 16.7 Million or better.

vi. Communications - 10/100/1000 Gigabit Ethernet (RJ-45).

vii. Ports & Connectors

viii. USB 2.0/3.0 = 2 minimum excluding the keyboard and mouse connections

ix. Gigabit Ethernet Port (RJ-45) = 1 or more. Display Port = 1 or more.

x. Power supply - 230 Volts AC, 50Hz, Built in power supply preferable.

xi. All-In-One (AIO) form factor is required with articulating stand.

xii. Sound bar with mic = 1 No.

xiii. System must not have any integrated Bluetooth and wireless adaptor.

xiv. Server and display should be from same OEM.

1. Software Configuration:

i. Protocols - RDP, PCoIP, Citrix, VMWare, view or other protocols required to support seamless remote access.

ii. Any device driver, protocol or license required to support the system **integration** to be provided by the vendor to complete the configuration.

iii. All in one thin client should be configured with embedded hardened OS which can support RDP/PCoIP to Servers with OS Windows Server 2022 or Latest version.

m. Scope of supply

Installation and Commissioning shall be included in the scope of supply.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*


रेलटेल
RAILTEL

14. Appendix 'N' – MCP Server and AIO Thin Client

M&C servers are deployed in BP1 & BP2 with 2 MCPs (Monitoring and Control Processors) and two GEIs (General Equipment Interface) in each station. These systems house the Monitoring and Control software that carries out schedule driven automatic configuration of the station as well as status monitoring of the station. Number of servers of GEI depends on the number of equipment deployed in the station. Current design of the software allows 50 equipment per GEI. The specifications for these servers are as below:

a. Processor –

i. Make & Architecture Intel CISC(X86-64),

ii. 24 Cores per processor,

iii. Processor Base frequency 2.6GHz,

iv. Processor Turbo Frequency 3.9 GHz,

v. Processor Description/ Number: Intel® Xeon® Gold 6542Y 2.9G, 24C/48T, dual socket configuration or equivalent

b. Chassis - Form factor Rack, Size 1 RU

c. **Motherboard -**

i. Chipset compatible with CPU Intel C741 or better

ii. Expansion Slots Gen 3 (PCIe x16) - 1 or more

iii. Minimum number of Sockets on Server - 2 or more

iv. Minimum number of Sockets populated with Processors on Server – 2 or more

d. Memory –

i. Type of RAM - DDR4 SDRAM with ECC

ii. Total Number of DIMM Slots - 32

iii. Minimum Number of DIMM Slots populated with DDR SDRAM - 2

iv. DDR SDRAM Size(GB) - 128

v. DDR SDRAM upgradable upto using spare DIMM Slots (GB) - 960

e. SSD Storage –

i. Type of Interface for SSD SAS

ii. Type of SAS SSD Mixed Use

iii. SAS SSD Hot Swappable Yes

iv. Endurance for SAS SSD (DWPD - Drive Writes Per Day) (X) 1

v. Total Number of Slots for SAS SSD 8

vi. Number of Slots shall populate with SAS SSD 2

vii. Minimum Capacity SAS SSD (GB) or more 1.92TB

viii. Total Capacity SAS SSD (GB) or more 3840

f. RAID –

i. RAID level 1

ii. No of RAID Controller Ports 8

iii. Speed of RAID Controller Ports (Gbps) 12

g. Ports & Interfaces

i. Network Card 1G,10G

ii. Number of Networking Interface Cards (LAN) 3

iii. Whether Network Interface Card Embedded No

iv. Total Number of Ethernet Ports required in Server 6x 1G, 2X10G

v. DVD-RW (Internal/External) Yes

vi. USB Ports (3.0) Minimum 3

vii. Total number of Spare Bays for Future Upgradation (Hot Pluggable) 8

h. Certifications –

i. Certifications/Compliance (OS) - Windows server 2022 Standard Edition ,Red Hat Enterprise Linux 9.4 or latest. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

ii. Compliance & Certifications – Following or equivalent international certification

iii. RoHS India [E-Waste (Management) Rules, 2016] certification

iv. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

v. Security Compliance – TPM 2.0, UEFI Secure boot

i. Operating System – Windows Server 2022 professional edition

j. **Management features**

i. IPMI 2.0 compatible management capability with dedicated management LAN

k. Generic

i. Redundant Power Supply - Yes

ii. Hot Swappable (Redundant Power Supply) - Yes

iii. Power Supply Efficiency – Platinum

iv. Redundant Fan - Yes

v. Hot Swappable (Redundant Fan) - Yes

vi. Server Main Supply - 230 +/- 10%Vac

l. All in one thin client (AIO) for Display & Remote access with Specifications as below:

i. Processor 2.5 GHz or above.

ii. System memory 8 GB DDR4 or above.

iii. Flash memory 256 GB PCIe NVMe SSD or above.

iv. Display 24 inch or above.

v. Display resolution - 1920 x 1080 FHD at 60 Hz, anti-glare or better and Color support 16.7 Million or better.

vi. Communications - 10/100/1000 Gigabit Ethernet (RJ-45).

vii. Ports & Connectors

viii. USB 2.0/3.0 = 2 minimum excluding the keyboard and mouse connections

ix. Gigabit Ethernet Port (RJ-45) = 1 or more. Display Port = 1 or more.

x. Power supply - 230 Volts AC, 50Hz, Built in power supply preferable.

xi. All-In-One (AIO) form factor is required with articulating stand.

xii. Sound bar with mic = 1 No.

xiii. System must not have any integrated Bluetooth and wireless adaptor.

xiv. Server and display should be from same OEM.

- *Software Configuration*

i. Protocols-RDP,PCoIP, Citrix,VMWare View or other protocols required to support seamless remote access.

ii. Any device driver, protocol or license required to support the system **integration** to be provided by the vendor to complete the configuration.

iii. All in one thin client should be configured with embedded hardened OS which can support RDP/PCoIP to Servers with OS Windows Server 2022 or Latest version.

m. Scope of supply

i. Installation and Commissioning shall be included in the scope of supply - Yes

n. Warranty

i. As per Warranty Terms of the RFP

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

15. Appendix 'O' – 75 inch large scale display

1. 75 Inch size Large LCD Monitor

a. Features

i.	Screen Size	:	75" or Higher LED Back Lit Panel
ii.	Panel Technology	:	up to 50 (Single side) or higher
iii.	Native Resolution	:	3840 x 2160 (UHD)
iv.	Brightness	:	500cd/m2
v.	Contrast Ratio	:	1100 : 1 or more
vi.	Dynamic CR	:	500,000 : 1 or higher
vii.	Operating System	:	WebOS
viii.	Orientation	:	Portrait & Landscape
ix.	Viewing Angle(H x V)	:	178 x 178
x.	Response Time	:	8 ms or better
xi.	Operation Hours	:	24 Hrs support

b. Connectivity

i. **Input Ports**

Digital	:	HDMI(3), Display Port(1)
External Control	:	RJ45(1), IR(1, Internal)
USB	:	USB -1
Audio In	:	Audio In-1

ii. AUDIO

Audio Power	:	20W(10W x 2)

c. **Additional feature** : Inbuilt : Internal Memory 16 GB, Wi-Fi, Screen Sharing feature, Web Link, Media Player, Picture in Picture & Picture by Picture feature (4 Simultaneously), SNMP Support

d. POWER

i.	Power Supply	:	100-240V~, 50/60Hz

ii. Power Type : Built-In Power

e. Certifications

i. (Safety/EMC/ER) : UL, FCC,BIS, RoHS

ii. Wall mount : Required

2. LCD Monitor Trolley Stand for 75 Inch

a. Features

i. Shall have Large and sturdy base

ii. Shall have base with Lockable Caster wheel

iii. Shall have Height-Adjustable Camera Shelf

iv. Shall have Internal cable management for the cable routing (Preferable)

v. Shall have Vertical Height adjustable display mounting bracket (minimum 3 levels)

vi. Shall have Tilting Adjustment (Preferred Tool less for quick viewing adjustment)

b. Technical Specifications

i. Dimension, Height x Width x Length (mm) (+/- 20mm) : 1840 x 680 x 1200

ii. Type : Heavy duty steel mobile LCD Display stand

iii. Screen Size : Shall support from 75 inch to 100 inch LCD Displays

iv. VESA Compatible : Shall compatible with VESA Mount dimensions of 200x200 to 1000x600

v. TV/Display Weight Capacity : Shall support Minimum 100kg

vi. Shelf Weight Capacity : Shall be Upto 20 KG

vii. Height Adjustment : Adjustable at three levels of 300/1380/1460mm (51.2"/54.3"/57.5") or equivalent or nearest slot level

viii. Tilt Range (Preferable) : +/- 10 Degrees

ix. Material : Steel structure with Black color powder coating matte finish

x. Certifications : CA 65 or equivalent

3. HDMI male to HDMI Male cable (10mtrs and 20mtrs)

a. Features

i.	Resolution	:	Cable to shall support 4096x2160 resolution @ 60 Hz
ii.	Data rate	:	18 Gbps or better
iii.	Colour depth	:	8 bits per colour
iv.	Wire Gauge	:	Copper wire with 22 AWG
v.	Standards	:	HDMI 2.0 or higher
vi.	Connector type	:	Male HDMI to Male HDMI
vii.	Contacts	:	Gold plated
viii.	Jacket	:	PVC
ix.	Regulatory compliance	:	UL CL

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

16. Appendix 'P' – Sys Log Server

1. *Rack Server – Configuration -2*

a. **Physical –** 19-inch rack mountable server of 1U rack mount size. Servers shall be offered with required rack mount hardware kit.

b. **Processor –** One Intel® Xeon® Silver 4510 (30M cache, 12 Cores, 2.4 GHz) or better or equivalent AMD processor on X86-64 architecture.

c. **Memory -** 128 GB ECC memory spread across all memory channels or better memory configuration.

d. **Internal Storage –** 2 Nos of 2 TB SATA Disk in RAID 1

e. **Drive Controller –** Internal RAID Card for RAID 1

f. **OS Certification:** RHEL & Windows certified hardware. All the required device drivers for RHEL shall be included in the offer. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

g. **Optical Drive –** Internal DVD RW drive to be offered

h. **Network Controller –** Total 4 nos of 1Gb Ethernet copper

i. **Ports –** Front :2 USB, Rear: 4 USB, VGA=1

j. **Power –**Hot Pluggable redundant power supply. Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

k. **Management -** Server shall include IPMI 2.0 compliant management module. Management function shall be offered on out of band over Ethernet.

l. **Cooling –** Server shall be configured with redundant cooling fans.

m. Certifications – Following or equivalent international certification

   i. RoHS India [E-Waste (Management) Rules, 2016] certification

   ii. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

   iii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

   iv. Security Compliance – TPM 2.0, UEFI Secure boot

n. **Operating System –** Redhat Enterprise Linux Server latest edition

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

17. Appendix 'Q' –SIEM Server

1. *Rack Server – Configuration -3*

a. **Physical –** 19-inch rack mountable server of 1U/2U rack mount size. Servers shall be offered with required rack mount hardware kit.

b. **Processor –** One Intel® Xeon® Gold 6548N Processor (60M cache, 32 Cores, 64 Threads, 2.80 GHz) or better or equivalent AMD processor on X86-64 architecture.

c. **Memory -** 512 GB ECC memory spread across all memory channels or better memory configuration.

d. **Internal Storage –** 10 Nos of 20 TB SAS 12G 7.2KRPM SAS Disk

e. **Drive Controller –** Internal RAID Card for RAID 1, 0, 10, 5 and 6 support with 8 GB Memory and 12G SAS interface

f. **OS Certification -** RHEL & Windows certified hardware. All the required device drivers for RHEL shall be included in the offer. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

g. **Optical Drive –** Internal DVD RW drive to be offered

h. **Network Controller –** Total 4 nos of 1Gb Ethernet copper and four numbers of 10Gb Ethernet Copper port shall be configured for each server.

i. **Ports –** Front :2 USB, Rear: 4 USB, VGA=1

j. **Power –**Hot Pluggable redundant power supply. Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

k. **Management -** Server shall include IPMI 2.0 compliant management module . Management function shall be offered on out of band over Ethernet.

l. **Cooling –** Server shall be configured with redundant cooling fans.

m. **Certifications –** Following or equivalent international certification

   i. RoHS India [E-Waste (Management) Rules, 2016] certification

   ii. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

   iii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

   iv. Security Compliance – TPM 2.0, UEFI Secure boot

n. **Operating System –** Redhat Enterprise Linux Server latest edition

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

18. Appendix 'R' – Colour Laser Printer

a. **Colour Laser Printer** : Duplex Colour Printing

b. Printer Functions

i. Print speed (Color and Black): 27 ppm or more.

ii. Duplex Print Speed (IPM) : 24 or better

iii. Paper Size : A4.

iv. Print Resolution : 600 x 600 or better

v. Print Technology : Laser

vi. Control Panel: 2-line backlit LCD graphic display; 5 buttons (Cancel, Select, Reverse, Right/Left arrows); LED indicator lights (Attention, Ready)

vii. Processor speed : 1200 MHz or better

viii. Memory : 512 MB or better

ix. Display : 2.7-inch(6.9cm) LCD with keypad or better

x. Durability Ratings/ Duty cycle: (No of Prints/month): 50000 or better

c. Connectivity

i. Standard connectivity : USB 2.0 port, Ethernet 10/100 /1000 (1 Gigabit Ethernet) network port

ii. Network capabilities : Yes (10/100/1000 Ethernet)

d. Paper

i. Input: 250 or higher100-sheet in main Tray, 50 or higher in Bypass Tray, 550 or higher in additional tray

ii. Yield of the cartridge/Ink Tank/Ink Pack supplied with Machine as per ISO/IEC - 19798/2007(E) for Cyan colour (Number of prints): 2100 or higher

iii. Yield of the cartridge/Ink Tank/Ink Pack supplied with Machine as per ISO/IEC - 19798/2007(E) for Yellow colour (Number of prints): 2100 or higher

iv. Yield of the cartridge/Ink Tank/Ink Pack supplied with Machine as per ISO/IEC- 19798/2007(E) for Magenta colour (Number of prints) : 2100 or higher

v. Yield of the cartridge/Ink Tank/Ink Pack supplied with Machine as per ISO/IEC-19752/2004(E) for Black colour (Number of prints) : 2400 or higher

vi. Duplex Print Options: Automatic (standard)

vii. Interfaces/Connectivity: 1 USB 2.0 Host ports; 1 Ethernet 10/100/1000 port

viii. Support Languages : PCL 6, postscript level 3 emulation, PDF

ix. Network Capability : 10/100/1000Base- Ethernet

x. Operating systems : Windows 10,11 and above; Windows Server 2016 and above 64-bit; Linux; Unix

xi. Power Supply : Built-in with power 230V +/- 10V AC 50-60 Hz

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

19. Appendix 'S' – Black and White Laser Printer

a. **Black & white Laser Printer** : Duplex Printing

b. Printer Functions

i.	Cartridge Technology	:	Composite Cartridge
ii.	Print Speed	:	up to 50 (Single side) or higher
iii.	Print resolution	:	1200 x 1200 or better
iv.	Type of Printing	:	Mono (Black & White)
v.	Cartridge Technology	:	Composite Cartridge
vi.	Duplex print	:	Automatic
vii.	Duplex Print Speed (IPM)	:	34 (two sided) or better
viii.	Print technology	:	Laser
ix.	Standard print languages	:	PCL 6, postscript level 3 emulation, native PDF printing (v 1.7)
x.	Printer management	:	Through Keypad

c. Connectivity

iii.	Standard connectivity	:	USB 2.0 port, Ethernet 10/100 /1000 (1 Gigabit Ethernet) network port
iv.	Network capabilities	:	Yes (10/100/1000 Ethernet)

d. Others

i.	Memory	:	512 or better
ii.	Processor speed	:	1.2 GHz or better
iii.	Duty Cycle	:	Up to 150000 pages monthly or higher
iv.	Paper Input :		550-sheet main input tray, 100-sheet in By pass Tray, 100-sheet Additional Tray
v.	Yield of the Cartridge pack supplied with machine as per ISO/IEC-19752/2004(E) for Black	:	5000 or higher
vi.	Paper / Media Size	:	A4, letter, legal, executive, envelopes
vii.	Operating systems support:		Windows 10,11 and above; Windows Server 2016 and above 64-bit; Linux; Unix
viii.	Display with Keypad:		2.7-inch (6.9 cm) LCD with keypad or better

ix. Power Supply : Built-in with power 230V +/- 10V AC 50-60 Hz

Note: Refer relevant sections for establishing compliance towards Warranty, Installation & System support, Quality Requirements and Notes to the Vendor for the offered product(s).

20. Appendix 'T' – NMS Software

a. **Network Management Software -** The NMS Software should meet following requirement–

   i. **Monitoring Network Matrices -** Incoming and outgoing traffic, Total bandwidth usage, Packet loss and interface error rates, Number of TCP connections, Link status, auto discovery of connected devices

   ii. **Monitor Health -** Interface speed and status, Device availability and uptime, CPU and memory statistics, Power supply status, Device information, Temperature sensors, Fan states, Create dynamic problem thresholds for different resource types (e.g. trunk port or uplink port)

   iii. **Generate Alert -** React to unexpected network spikes, errors, packet loss, or ping loss; Analyze long-term bandwidth usage trends; Suppress alerts while performing device maintenance or upgrades; Dynamically detect anomalous network behaviour

b. Server Monitoring

   i. **Server performance -** High CPU or memory utilization, Network bandwidth usage, Packet loss rate, Interface error rate, Number of TCP connections is anomaly high for this day of the week, Aggregate throughput of core routers is low

   ii. **Server availability -** Free disk space is low, System status is in warning/critical state, Device temperature is too high / too low, Power supply is in critical state, Fan is in critical state, No SNMP data collection, Network connection is down

   iii. **Configuration changes -** New components added or removed, Network module is added, removed or replaced, Firmware has been upgraded, Device serial number has changed, Interface has changed to lower speed or half-duplex mode, out of the box template to monitor popular server and OS

c. **Service Monitoring –** Capability to monitor services in REHL and Windows OS.

d. **Application Monitoring** – Capability to monitor standard and integrate for custom application monitoring

e. **Log Monitoring** - Detect warning and error messages generated by an application, Receive alerts on security incidents by monitoring security logs, Visualize and graph the number of logged events

f. The platform shall have more than 300 internal templates built in for identification of popular products. Shall have Out of the box monitoring for leading software and hardware vendor.

g. The software shall support out of the box integration with leading ITSM systems

h. The monitoring software must be deployed on RHEL platform.

i. The monitoring software shall have agent for windows and linux hosts. The solution shall also have template for Proxmox Virtual Environment Monitoring.

j. **Support** – The monitoring software infrastructure should be upgraded to latest version once in a year or based on required upgrade based on latest features as required. All the implementation shall be migrated to new platform whenever such software upgrade is carried out. Vendor shall ensure all the configuration is migrated from existing platform to new platform during platform migration.

k. **License requirement** – The NMS platform shall need to monitor 35 Network Device (Including Switches and Routers), 160 hosts (including HCI infra, host and VM), 30 services and 30 applications. Suitable license shall be offered

Note: Refer relevant sections for establishing compliance towards Warranty, Installation & System support, Quality Requirements and Notes to the Vendor for the offered product(s).

21. Appendix 'U' –KVM and RKM

1. The quantity and specification of KVM and RKM are as mentioned below:

a. **Quantity**

i. No of IP console switches (KVM) = 1

ii. No of RKM Units = 2

iii. No. of USB interface adapter for KVM = 40

iv. No. of Serial Interface Adapter to Connect COM Port of Network/Servers for KVM=10

v. No. of Virtual Media Interface Adapter=01 No

vi. RKM, KVM and Adapters shall be of same OEM Make.

b. Specifications for KVM Switch (Config 1):-

i. No. of Target device ports per unit= 40 as a single unit (with out cascade)

ii. Supports up to 4 users as remote users over IP KVM Session and 1 local user

iii. Device shall have dual power supply

iv. Device shall have two NIC ports

v. Advanced FPGA graphics processor with HD resolutions up to 1920 x 1200

vi. High Video Resolutions – up to 1920 x 1200 @ 60 Hz with 24-bit color depth at the switch's local console and on remote displays

vii. Laptop USB Console (LUC) – a dedicated USB port directly connects to a laptop for easy console operation

viii. Supports PS/2, USB, Sun Legacy (13W3) and serial (RS-232) connectivity

ix. Local console provides USB keyboard and mouse support and same OEM make as the offered RKM

x. Supports multiplatform server environments: Windows, Mac, Sun, Linux and VT100 based serial devices

xi. Critical system event notification via SMTP email; SNMP trap and Syslog support

xii. IPv6 capable

xiii. Supports TLS 1.2 encryption and RSA 2048-bit certificates to secure browser logins

xiv. Virtual media enables applications, OS patching, software installations and diagnostic testing

xv. Console port - 2 x USB Female (Black) 1 x DVI-I Female (White)

xvi. Form-Factor: 1U Height with 19" Rack Mountable Option

xvii. Remote virtual media - Easily load and update software and firmware from anywhere on the LAN or WAN when used with Virtual Media Interface Adapters.

xviii. Internal dual power supply with rated Voltage 100 to 240V AC at 50 to 60 Hz should be offered

c. Specifications for KVM Switch (Config 2):-

i. No. of Target device ports per unit= 8 as a single unit (with out cascade)

ii. Supports up to 4 users as remote users over IP KVM Session and 1 local user

iii. Device shall have dual power supply

iv. Device shall have two NIC ports

v. Advanced FPGA graphics processor with HD resolutions up to 1920 x 1200

vi. High Video Resolutions – up to 1920 x 1200 @ 60 Hz with 24-bit color depth at the switch's local console and on remote displays

vii. Laptop USB Console (LUC) – a dedicated USB port directly connects to a laptop for easy console operation

viii. Supports PS/2, USB, Sun Legacy (13W3) and serial (RS-232) connectivity

ix. Local console provides USB keyboard and mouse support and same OEM make as the offered RKM

x. Supports multiplatform server environments: Windows, Mac, Sun, Linux and VT100 based serial devices

xi. Critical system event notification via SMTP email; SNMP trap and Syslog support

xii. IPv6 capable

xiii. Supports TLS 1.2 encryption and RSA 2048-bit certificates to secure browser logins

xiv. Virtual media enables applications, OS patching, software installations and diagnostic testing

xv. Console port - 2 x USB Female (Black) 1 x DVI-I Female (White)

xvi. Form-Factor: 1U Height with 19" Rack Mountable Option

xvii. Remote virtual media - Easily load and update software and firmware from anywhere on the LAN or WAN when used with Virtual Media Interface Adapters.

xviii. Internal dual power supply with rated Voltage 100 to 240V AC at 50 to 60 Hz

should be offered

d. Specification for RKM Units

i. **Specification**

1) 1U rack-mountable with integrated monitor, keyboard & mouse functionality
2) Rail Type: Dual Rail
3) Shall be of same make of OEM for KVM units
4) Input Video Resolution up to 1920 x 1200 @ 60Hz
5) Mode (Output) 1920 x 1080 @ 60Hz
6) Compatible with Windows and Linux
7) **Keyboard/Mouse Emulation:** USB connectors
8) No of VGA IN Ports=1
9) No of HDMI = 1 No
10) Monitor shall be mounted inside the foldable lid that covers the keyboard
11) Keyboard shall have minimum 88 Keys layout including trackball mechanism for smooth navigation in the base.

ii. Display Type:

1) Flat-panel, LCD
2) 18.5" TFT-LCD or better
3) Maximum Input Graphics Resolution 1920 x 1080 @ 60Hz
4) Response time <25ms
5) Contrast ratio – 1000:1
6) Viewing Angle : 178
7) Color : 16.77M colors
8) Luminance >= 300(cd/m^2)
9) On Screen Display (OSD) Controls should support English language and should provide option for Brightness, contrast, positioning, color temperature, individual color control, input selection, factory reset

iii. Certification and Compliance

1) ROHS
2) Energy Star Compliant

e. **USB Interface adapter for KVM:** USB interface Adapter is required to connect End- Devices, specifically Servers with VGA-Out and not having PS2 Keyboard and mouse ports to the KVM console Switch.

f. **Serial Interface adapter for KVM:** To connect Serial port devices over 9-pin serial console port to KVM switch.

Note: Refer relevant sections for establishing compliance towards Warranty, Installation & System support, Quality Requirements and Notes to the Vendor for the offered product(s).

22. Appendix 'V' – SIEM Software with 3500 EPS

SIEM (Security Information and Event Management) Solution: solution for 3500 EPS or 100GB per day data license capacity.

a. Requirement

i. The solution shall be delivered as a VM ready solution deployable over KVM or equivalent virtualization platform. If the solution requires proprietary VM infrastructure, vendor shall include the required licenses for VM platform.

ii. The solution shall be deployed as a multimode server cluster may be delivered as a native or offered as a third party solution. Any license requirement shall be offered by the Vendor.

iii. The solution shall be deployed with purpose-built operating system. In case the solutions use generic operating system platform it must be limited to only Linux or Debian.

iv. The offered platform shall have following compliances –
1) SOC -3 Compliant product
2) ISO 27001, ISO 27017 and ISO 27018 compliant
3) Support Section 508 compliance

b. General

i. The solution shall offer enterprise-grade security and developer-friendly APIs to machine learning and graph analytics with features to ingest, analyse, search, and visualize all types of data at scale.

ii. The solution shall be highly scalable cluster as a collection of one or more nodes (servers) that together holds all of data and provides federated indexing and search capabilities across all nodes. The cluster set also provides availability by providing features like failover. Internal rebalancing occurs every time a node exits or join the cluster to provide distribution of data.

iii. The offered solution shall be horizontally scalable as demand increases. The platform shall support cross cluster replication which is rack aware and site aware.

iv. The solution shall have visibility into platform environment and can control how long the data set to be retained with the environment.

v. The solution shall be manageable via variety of management tools including UIs, APIs etc.

vi. The solution shall allow the administrator to define the Index life cycle management and define Hot, Warm, Cold/Frozen and Delete operation on the Indexes. The solution will allow to create data Tiers (Hot, Warm, Cold) accordingly.

vii. The solution shall have native snapshot capability to protect its data from accidental modification. The snapshots can be stored in a repository on a shared file system. The solution shall have capability to directly query the snapshots. The snapshot life cycle management capability shall also define the lifecycle of the snapshot provide native with the platform.

viii. The solution shall support snapshot based peer recoveries.

ix. The solution shall provide features like data rollup which will create only summary of actual data and discard detailed data.

x. The solution shall support data ingest capability via Data Stream.

xi. The solution shall provide CLI tools for managing the interface along with Web UI for the same.

xii. The solution shall provide suitable Upgrade UI which will assist to identify the deprecated settings in your cluster and indices, guiding you through the process of resolving issues — including re-indexing.

xiii. The solution shall allow to create user and roles via API and UI.

xiv. The solution shall support representing data in Transforms and directly digestible for ML.

xv. The platform shall provide full stack alerting mechanism (for email, IBM Resilient, Jira, Microsoft Teams, PagerDuty, ServiceNow, xMatters, and Slack. Integrate with any other third-party system via a weblook output)for events and query based results

xvi. The solution shall provide control of the alerts by viewing and managing all of them from a single UI. It shall provide features for alert suppression and noise reduction in UI mode. It shall support alerts based on triggers like incidents satisfying internal rules.

xvii. The solution shall have access rights mechanism to provide granular access to users on control their rights on data and operation. The solution shall support Role-based access control (RBAC) and Attribute-based access control (ABAC). Internal keystore (password protected) mechanism shall provide additional layer of security.

xviii. The solution shall use encrypted communication channel between nodes using SSL/TLS

xix. The solution shall provide easy sharing mechanism of dash board with anonymous users without compromising security of the infrastructure.

xx. The solution shall have field-level security which restricts the fields that users have read access to. It shall restrict which fields can be accessed from document-based read APIs.

xxi. The solution shall support security features like audit logging, IP filtering, Security

realms , Single Sign on, third party security integration

xxii. The offered solution shall support Section 508 compliance standards and shall meet to meet Section 508 compliance standards.

xxiii. The offered solution shall support working on data anywhere with RESTful APIs, language clients, robust DSL

xxiv. Data ingestion: Solution shall collect security events and logs from various sources, including network devices, endpoints and third-party security tools. It shall support following device and application context

1) Network Devices including Switches, Routers, Wireless LAN
2) Security devices — Firewalls, Network IPS, Web/Email Gateways, Malware Protection, Vulnerability Scanners
3) Servers including Windows, Linux, MAC
4) Infrastructure Services including DNS, DHCP, DFS, AAA, Domain Controllers, VoIP
5) User-facing Applications including Web Servers, App Servers, Mail, Databases
6) Cloud Apps including AWS, Box.com, Okta, Salesforce.com
7) Virtualization infrastructure including VMware ESX, Microsoft Hyper-V Scalable.

xxv. Advanced analytics: The solution shall provide machine learning and advanced analytics techniques to identify anomalies, patterns and potential threats in the collected data. The platform shall allow searching features as follows -

1) Search events in real time— without the need for indexing
2) Keyword and event-based searches
3) Search historical events — SQL-like queries with Boolean filter conditions, group by relevant aggregations, time-of-day filters, regular expression matches, calculated expressions — GUI and API
4) Use discovered CMDB objects, user/ identity and location data in searches and rules
5) Schedule reports and deliver results via email to key stakeholders
6) Search events across the entire organization, or down to a physical or logical reporting domain
7) Dynamic watch lists for keeping track of critical violators — with the ability to use watch lists in any reporting rule
8) Scale analytics feeds by adding Worker nodes without downtime

xxvi. The solution shall support scalable and flexible log collection. The features shall support -

1) Collect, Parse, Normalize, Index, and Store security logs at very high speeds
2) Out-of-the-box support for a wide variety of security systems and vendor APIs — both on premises and cloud
3) Windows Agents provide highly scalable and rich event collection including file integrity monitoring, installed software changes, and registry change monitoring

(Process, file, network, DNS, driver and DLL loads, registry, malware security detections)

4) Linux Agents provide file integrity monitoring, syslog monitoring, and custom log file monitoring (Process, file, network)
5) Modify parsers from within the GUI and redeploy on a running system without downtime and event loss
6) Create new parsers (XML templates) via integrated parser development environment and share among users via export/import function
7) Securely and reliably collect events for users and devices located anywhere

xxvii. The solution shall support active agents on hosts which shall work as Detection engine, Timeline, Cases and administration of hosts that runs active agents

1) Active Agent: Automatically searches for unusual network and host activities using:
    - Detection rules: Regularly scan data from the hosts for abnormal events. When a suspicious event is found, the engine generates an alert.
    - Exceptions: Decrease noise and false positives by associating exceptions with rules, preventing alerts when exception conditions are met. Value lists include source event values that can serve as part of the exception conditions.
    - Machine learning jobs: Automatically detect anomalies in network and host events. Anomaly scores are given for each host and can be combined with detection rules.
    - Timeline: A workspace for examining events and alerts. Timelines employ queries and filters to probe into events related to specific incidents.
    - Cases: An in-app system for opening, sharing and tracking security issues within the Security application. Cases can be integrated with a ticketing system.
    - Administration: Monitor and manage hosts that run active agent

xxviii. Incident response and case management: The platform shall include case management features that help security teams to organize and manage security incidents. This streamlines the incident response process, enabling teams to collaborate more effectively and resolve security issues faster. The features include -

1) Automation and Incident Management
2) Policy-based incident notification framework
3) Ability to trigger a remediation script when a specified incident occurs
4) API-based integration to external ticketing systems
5) Built-in Case Management system
6) Incident reports can be structured to provide the highest priority to critical business services and applications
7) Incident Explorer — dynamically linking incidents to hosts, IPs and user to understand all related incidents quickly

xxix. Real-time monitoring: The solution shall allow security teams to monitor security events, manage logs and receive real-time alerts, providing a comprehensive and up-to-date view of an organization's security posture.

xxx. The solution should have ability to leverage MITRE ATT&CK Framework integration within events\incidents (ID, Tactics, Technique). The solution repository should have Activity data as well as Detection data (which should be mapped to MITRE TTPs framework)

xxxi. Customizable dashboards: The solution shall provide pre-built dashboards and visualization tools which enabling security teams to create custom views and visualizations of security data.

xxxii. Alerting and notifications: The offered solution shall provide a flexible alerting system that allows security teams to create custom rules and receive notifications on potential threats. This helps ensure that teams are promptly alerted to critical security incidents.

xxxiii. Threat hunting: The offered solution shall enable proactive threat hunting by providing powerful search and analytics capabilities, allowing security teams to investigate potential threats and uncover hidden patterns.

xxxiv. Support – Vendor must offer OEM support for single node implementation for the support duration.

23. Appendix 'W' –Network Behavior Analytics (NBA/NBAD)

a. The solution should be an appliance based solution – delivered as an OEM certified appliance as an integrated package.

b. The solution shall have collector or sensor and analytics as two different component for flexible deployment in the existing network, with-out changing any configuration in the network. It shall be possible to control the analytics node from a master node/ central node for monitoring and configuration.

c. The collector shall have capability to keep raw data for 3 Days and normalized data for 100 days locally. Beyond 100 days the normalized data/metadata to be pushed to central syslog.

d. The license capacity of the traffic must be calculated based on average throughput of 7 days and not by peak throughput of the interface. The license capacity must ensure total average throughput of 5 Gbps full-duplex when aggregated across all the network segments and must not pose limitation based on network segment.

e. The networks for which the details are shared above shall have overlapping IP address range. The solution must support working with overlapping IP addresses, keeping context of the network preserved.

f. The solution should be on premise and should not require internet access for day to day functionality. Any required update should be supported offline.

g. The solution must be an out of band analytics engine from the primary data path.

h. The solution shall be designed along with its associated component as a monitor only capability to ensure no data is ingested in critical network. Suitable datasheet and hardware details to be shared with the offer.

i. Throughput – The product must be licensed for total 7 Gbps average throughput

j. The solution must be designed to collect data from three networks minimum per site as follows –

   i. Network X – Directly connected on the NBA platform with 3 Gbps Full Duplex span/mirror traffic

   ii. Network Y – Connected via isolation mechanism (Isolation at Layer -1) to ensure only one way traffic is ingested to the NBA with 1 full duplex Gbps Span traffic

   iii. Network Z – Connected via isolation mechanism (Isolation at Layer -1) to ensure only one way traffic is ingested to the NBA with 1 Gbps full duplex Span traffic

k. The vendor shall provide detailed design to ensure the isolation mechanism is established in the media and not on higher layer (Layer 3 or higher). If the isolation is achieved in higher layer (Layer 3 or more) then the offer will be technically rejected.

l. The solution must be able to maintain the context of the network where the data is collected.

m. The solution must be able to analyze and forward extracted metadata to syslog. This syslog data must be ingested to the SIEM for further analysis

n. The sizing of the solution must match traffic aggregation bandwidth criteria as mentioned above.

o. The solution must capture live span/port mirror traffic of the network of interest and shall be able to capture the data.

p. Proposed NBA/NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc

q. Responsibility of configuring the switches for successful deployment of proposed NBA/NBAD systems lies with the supplier

r. The solution should maintain an updated 90-day profile (minimum) of all devices including a summary of protocol history to aid in the discovery of low-and-slow attacks.

s. The solution should provide contextual network-wide visibility via completely agentless approach.

t. The NBA/NBAD tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NBA/NBAD integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.

u. The solution should provide an independent and comprehensive analysis of the attack surface by uniquely identifying and profiling endpoints (Windows, MacOS, Proxy machines, Phones, Printers, IoT, etc.) based on behavioral fingerprints irrespective of IP address changes.

v. The solution must support minimum 20 ML models for enhanced detection and should not rely on only Rules/IOCs for threat identification.

w. The solution using AI-driven security must be able to autonomously build a case management collecting artifacts on its own and attaching them to the case management without any human intervention.

x. The solution should support and provide examples for minimum two of the , of the following data science methods. Details with examples on how each of these data science methods are used should be provided and demonstrated as part of the proof of concept evaluation if required (corresponding ML model to be provided).

   i. Supervised machine learning
   ii. Unsupervised machine learning
   iii. Deep neural networks
   iv. Belief propagation
   v. Multi-dimensional clustering

vi. Decision tree classification

vii. Outlier detection

y. The solution should be able to provide real-time monitoring and visibility into all network traffic, using machine learning, context-aware analysis, and on-premise threat detection and analytics.

z. The solution shall use behavioral technology and machine learning and advanced entity modeling to reduce false positives. Solution should detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.

aa. The solution must fully expose the definitions for all out of the box vendor provided threat detection techniques (models/Rules/ML/etc) and allow for their easy modification or adaptation.

bb. The NBA/NBAD solution should also offer the flexibility and capability to drill down into the end user, MAC, flows, interface utilization and a wide array of other host statistics needed for rapid incident resolution. Should utilize anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration.

cc. The solution should be able to natively identify the fingerprints from network traffic including but not limited to domains, ciphersuites exchanged in TLS handshake, HTTP body hash etc. All the fingerprints which uniquely identify the devices should be clearly grouped together and provide count of the times the fingerprints were seen on the network.

dd. The solution should detect threats in encrypted traffic without the need to decrypt or only comparing JA3 hash values. For example, the solution should check the commonality and frequency of TLS ciphers and destinations, without requiring support from existing network switches, endpoint agents, network proxies or threat intelligence feeds.

ee. By collecting, analyzing and storing available log information from various sources, NBA /NBAD System should provide a full audit trail of all network transactions for detecting anomalous traffic and performing more effective forensic investigations.

ff. The solution should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.

gg. The solution should provide use cases to identify usage of insecure, legacy and deprecated encryption algorithms being used by servers on the network.

hh. The solution must detect unusual, unauthorized behavior within the network. This includes but is not restricted to unusual RDP, port scanning, unauthorized new devices plugged in, unauthorized use of access credentials to internal resources.

ii. The solution should have DNS Threat Analytics Capability to detect the threat present in DNS traffic, DNS spoofing and DNS tunneling attack.

jj. The solution should highlight weak ciphers being used in the network by hosts or applications. The solution should search and monitor cipher suites and report on which ones are used on the network.

kk. The solution should be capable of rejecting particular network data from analysis using input filters. For example, exclude Video surveillance data from being processed by the NBA/NBAD solution

ll. The solution must support VPN tunnel detection for private and anonymous VPN tunnels and just not the VPN used by the Organization. Privacy VPN - Personal VPN solutions which enable the user to avoid network monitoring solutions

mm. The solution must support port-agnostic protocol detection. The Solution must be capable of conducting protocol analysis to detect applications using unexpected ports, anomalous transfer of data via certain protocols indicative of tunneling activity, backdoors, and the use of forbidden application protocols

nn. The solution must provide support for various OT protocols such as modbus, profinet, cip, bacnet_app,opcua, iccp, honeywell_phd,s7comm, bacnet_net,pccc, iec104, dnp3, goose, vnetip, bacnet_vlc, deltav, mqtt, etc. Minimum 10 OT protocol must be listed in datasheet.

oo. The solution must distinguish between similar devices based on unique fingerprints (including unmanaged & IOT) and provide commonality & frequency analysis for each such fingerprint to minimize the false positive rate. Must automatically group similar devices together based on a combination of fingerprints, provide an explanation of the similarity, and identify packet captures corresponding to that fingerprint for forensic and outlier analysis.

pp. The solution should identify the presence of botnets in the network. and detect long-lived connections that may be associated with data-exfiltration.

qq. The solution must provide APIs to integrate with existing security solutions like Security Information and Event Management (SIEM), Next-generation Firewalls, Router, Switches, NAC, SOAR, Proxy, WAF, Mail gateway etc. Necessary applicable licenses for integration with other security devices must be supplied from day one

rr. The solution should support all the following features without exception, under the incident management workflow component with built-in automation that automatically:

i. Visually maps out the devices and external destinations involved in the incident

ii. Visually maps the relationships between the devices involved using machine learning and not solely based on simply correlating all connections to a known malicious IP or domain.

iii. Use natural language processing and topic modelling to add context to the incident

iv. Provide a complete audit of the automated investigation.

v. Mark legitimate activities of the devices involved during the time of the incident

vi. Suppress activities that are not relevant to the attack automatically.

vii. Automatically generates an incident of the attack when new traffic is added.

viii. Provide a PDF report of the incident.

ss. The solution should have capability to assign risk and credibility rating to alerts and hosts and present

critical high-fidelity alerts prioritized based on threat severity with contextual

information on the dashboard.

tt. For each and every device that uses multiple IP addresses due to DHCP over a period of time, the system must display all the previous IP addresses linked to this device on the GUI along with the most recent IP address assigned to the device.

uu. The solution must show on the GUI when the device was first seen for all the devices being monitored by the system along with the last active timestamp.

x. The solution should have integration with the MITRE ATT&CK matrix and also should mandatorily show the suggested mitigation recommendation for each of the TTPs in ATT&CK matrix.

ww. The system should have a mechanism to consume external lists of known bad IP's and generate alerts on the same if connection is seen.

xx. The solution should also have the capability of threat intelligence management where the custom threat intel IOCs can be added by the user

yy. Storage Calculation – The total storage for the solution must be computed as follows -

i. Average Packet Size (Raw and Metadata) – 576 Bytes

ii. Total Numbers Packet in the 5 Gbps full duplex Link – 1785714 (Considering 80% capacity in full duplex mode)

iii. Number of Days of Storage Required for raw Data – 3 Days

iv. Number of Days of Storage Required for Meta Data – 100 Days

v. Link Utilization considered – 100% full duplex

vi. Raw data Storage –240 TB, If OEM support compression proportionately reduction in storage shall be considered. However, suitable datasheet or evidence to be provided.

vii. Meta data Storage – 75 TB, If OEM support compression proportionately reduction in storage shall be considered. However, suitable datasheet or evidence to be provided.

24. Appendix 'X' – One time Implementation and Documentation

1. System Integration, Implementation, Service Migration and Security Audit

a. **General Instruction -** Vendor shall carefully go through the scope of system installation, service migration and security audit requirements and accordingly propose the solution:

i. Vendor to note that, as user site is an operational setup and vendor needs to deploy and migrate operation to new hardware, Vendor must prepare step by step plan of system deployment/implementation and service migration activity.

ii. Vendor must make a rack layout plan and work out how the old hardware will be removed and new hardware will be integrated in the rack along with service migration. The integration and migration activity involves existing 12 nos. of 42U standard racks. Vendor must note that all the deliverables may not be accommodated in the server rack without removing the old hardware from the operation. Hence a sequence of planned migration must be worked out by the vendor. The same needs to be presented to NSIL/User team.

iii. Vendor must note that, the planning activities on system implementation and service migration activity may start prior to the actual hardware delivery to reduce the installation and implementation timeline.

iv. This may be noted that, Vendor team has to study the existing configuration and make detailed migration plan document and present it to NSIL/User Team for plan review and approval. It is responsibility of vendor to migrate operations without extra downtime

v. Vendor shall ensure for each specific activity, expertise in skills are available on site for system implementation and service migration activity

vi. It may be noted that, for any service migration task, maximum two hours downtime will be acceptable and will be provided as a continuous span of two hours during any time of the day in concurrence with NSIL/User. The migration process must have plan for each network component, time split-up with respect to activity wise, considering fall back scenario for each service migration.

vii. It may be noted that vendor will be provided access to the existing setup (in read only mode) to understand the configuration of each element and workout the service migration plan. It is responsibility of the vendor to understand various dependencies in the configuration and perform successful migration of service without disrupting the existing operation. Vendor should build required test setup to demonstrate the User/NSIL team on success of the plan before implementing at actual wherever required. Each service migration will be examined in operation for final acceptance by

User/NSIL team.

viii. Vendor may note that the section below broadly describe the scope of work. However the delivery will not be limited only to mentioned points. NSIL/User may ask to implement any of the features which are part of product specification and required for NSIL/User implementation. Ex. WORM feature for Storage, Virus Scanning Feature for Storage, and File system audit configuration for storage. Considering this fact, vendor must review the product capabilities asked and shall support delivery of and to demonstrate of suitable features during product implementation.

b. **Service Migration:** Vendor shall carry out following service migration activity:

i. **LDAP/NIS:** Understand the existing implementation of LDAP/NIS and hosting new LDAP infrastructure. Migration of user database and attributes to newly hosted LDAP server and successful demonstration of operation of User control center with new LDAP. Vendor shall also implementation the recommended security hardening based on the OS platform and application software. The migration will be functionally accepted when User operation is successful for twenty four hours even after shutting down of the existing (old) LDAP/NIS severs.

ii. **Storage and Backup:** Understand the existing implementation of storage and backup policy and accordingly create required aggregates, volumes , snapshots and file system on the new storage. Migration of data to the new storage with-out changing the attribute of data types. Vendor shall use suitable data synchronization tools/software's to ensure the file attributes are not changed during synchronization process. The backup configuration shall ensure current backup features are available. Vendor shall also implementation the recommended security hardening as per OEM recommended practices for Storage and Backup environment. The migration will be functionally accepted when User operation is successful for twenty four hours even after shutting down of the existing (old) Storage Servers.

iii. **Operation migration of FTP/SFTP and Rysnc Configuration:** Vendor shall study the configuration of FTP/SFTP and Rsync host / service configuration and replicate the same configurations on new hardware on latest version of operating system along with security hardening (SELinux, Host Firewall etc). The FTP log shall be configured in vivid mode to record essential details. The migration will be considered successful once the operation is successful for twenty four hours even after shutting down of the existing (old) systems.

iv. **Migration of Real-time Distributors:** Configuration of Realtime data Distribution system will be provided on new hardware by providing identical network configuration of the system along with all the required hardening. NSIL/ISRO/User team shall migrate the application software to new data

distribution server. There will be two such servers in the configuration and migration shall be done one by one on different working days. NSIL/ISRO/User application team will verify the success of the migration.

v. **Syslog Service Migration:** Configuration of SysLog server will be carried out based on existing configuration and shall be integrated with all the elements with proper log organization and rotation. The Syslog host will be provided with 1TB NFS area which will be only mounted for Syslog node in read-write mode and will be available to other nodes (if required) in read-only mode. This configuration shall be restricted from Central NAS storage. The migration will be considered successful after verification of all device log getting recoded in the new hardware for two days after shutting down the existing (old) system. The required configuration to push Syslog to the Syslog server needs to be configured in entire pool of systems (Router, Switch, server, Workstation, Tape Library, SAN Switch, VMs etc) as part of implementation.

vi. **Ansible Service –** Vendor needs to migrate the Ansible implementation to the new infrastructure on latest version of the software. Vendor also need to add new playbook as and when required.

vii. **NGFW Migration -** Configuration of UTM Device shall be carried out by deployment of UTM manager with suitable internet connection (As per provided connection by User) and integrating the UTM with Manger for configuration management patch update. The UTM Manager and Analyzer Device shall be updated to latest stable version before configuration of UTM Device. The vendor shall review the configuration of existing UTM and build the policy accordingly in the new UTM keeping the resource, service and groups name identical. Vendor shall ensure the services are built with suitable controls of IPS, IDS and Antivirus feature and shall successfully demonstrate detection of malformed traffic if attempted to transfer via the interface. The physical interfaces shall be labelled as per requirement. Once all the policies are built, it will be reviewed by User/NSIL team and shall be given authorization for migration of the services. The UTM overall environment will be monitored for two working days for complete review of Manager, Analyser and traffic flow behavior and declare as complete. Vendor may also note that, the new UTM may need creation of additional partition for integration of ground station M&C network to the same device. Required policies and guidelines shall be provided by User team during implementation. The vendor shall also integrate the Enterprise End Point Management System (EMS) and end point protection software with the security fabric and enable suitable policies for identified endpoints.

viii. **Router configuration–** The routers are deployed at User Control Center and other interfacing locations. Vendor needs to study the configuration of the existing (old) routers and replace the configuration with new router hardware. The vendor shall ensure the router firmware is updated to latest version of

the image/firmware before deployment. Where ever required, IPSEC tunnels will be established with QoS (Quality of Service) and required VRFs will be created for service isolation as per NSIL/ISTRAC/User requirement. Vendor shall also ensure the recommended security configuration for the router will be implemented as per OEM best practices and guideline. The User team shall verify the configuration and observe successful operation for two working days before acceptance of the configuration.

ix. **Switch configuration -** Vendor shall ensure the all the existing switches will be replaced by newly delivered switches and configuration will be ported to the new hardware. All the switches shall be placed on latest version of stable firmware as per OEM recommendation before deployment. The switches shall be security hardened as per OEM recommendation. Vendor shall also enable 802.1x (port security) as per requirement of User team. The User team shall verify the configuration and observe successful operation for two working days before acceptance of the configuration.

x. **RKM and KVM -** The vendor shall integrate the RKM and KVM infrastructure with the newly delivered elements and connect all the equipment to the management port as per requirement. The management network will be a completely isolated network from data network. The management interface shall be used for update of firmware and device drivers for various hardware elements wherever feasibility exists. The User team shall verify the integration process and observe successful operation for two working days before acceptance of the configuration

xi. **Management Interface -** Vendor shall study the management configuration interface and bring all the devices with management port to a single management network fabric. Vendor shall ensure that the management LAN shall be deployed with a LDAP Server / VM and users shall have dedicated named account for access of Management Interface. Every device shall have read-only and super admin account and shall be mapped to user roles. The management LAN shall also have syslog configuration for collecting event logs from each hardware.

xii. **Workstation Configuration -**Vendor shall install the latest RHEL packages as per provided package list and shall ensure the Nvidia drivers and associated configurations are configured.

xiii. **Host/VM Host Environment Configuration:** Vendor needs to install RHEL OS in respective hosts (server, workstation, VM instance for total around 150 nodes/instances) and shall configure the following

1) Operating system installation and registration/ activation wherever required.
2) Device driver installation
3) Dual-display configuration (only for few workstations)
4) Network and timing configuration

5) NIS/LDAP Client, Network and Channel Bonding and NFS configuration
6) SELinux, Host Firewall and Peripheral Device control policy implementation
7) FAPolicy configuration

c. **System Implementation:** The following new interfaces will be implemented by the Vendor as per detailed requirement. The detailed requirements will be provided by User/NSIL team and accordingly vendor has to prepare plan of implementation along with details of resources, network plan, interconnect diagram etc for approval by User/NSIL team. Vendor shall ensure sufficient care taken to avoid any disruption in operation during the process of Implementation.

i. **Data Diode:** Vendor shall configure the data diode (provided by NSIL) for movement of files from external network to internal network via Data Diode1 and Internal network to External Network via Data Diode2. While a file is copied from External network to internal network, the file will be scanned via antivirus software before further movement to the internal network. The interface system in the internal network will be made as a staging system where the Anti-Virus engine will scan the file before further delivery to the internal path. The completion of this interface shall be verified by moving files in and out of the User LAN via data diode interface. Vendor may note that the data diode hardware will be provided by NSIL along with configuration guide. Vendor has to provide the integration and antivirus / host protection software configuration along with file delivery path.

ii. **End Point Protection and Control:** Vendor will establish the Antivirus Central server infrastructure which will be deployed in User internal network and shall provide virus protection for all the FTP server, Data Diode interface server and any other node which is required for protection. The Vendor shall make arrangement via data diode interface to bring regular database updates for the anti-virus engine or via integration with NGFW Fabric. The success of the implementation shall be verified by successful detection of the test malware placed by User team during acceptance and through verification of the automatic update process.

iii. **Monitoring Dashboard:** Vendor shall configure monitoring dashboard using the management and monitoring software as follows –

1) Network WAN View –This view shall show the live status of connectivity with User and other entities with the description of the links. With this dashboard view, operations team shall make out any connectivity issues (on WAN) and shall represent live status of the link in healthy, degraded or down mode.
2) Network LAN View – This view shall show the critical LAN switches and UTMs and also exhibit health status of the device with respect to any internal failure, This configuration shall monitor the critical interconnection status like core switch to Mission Storage or core switch to core switch interconnect etc. User team shall provide the functional requirement of the LAN view.

3) View for Real-time and Offline Service/Application Status – In this view the critical real-time and offline Services will be shown along with system / hardware health and also the service health. Critical service information will be provided to the implementation team for making the required configuration.
4) Security View – This dash board will show the status of critical security function like Antivirus, SIEM, Ansible etc and its running status.
5) Complete LAN view – This will be a discovery view which will list complete topology and every connected device should be visible with in User LAN under this view.
6) The views will be placed in a cyclic view in one screen and in dedicated view in other screens as provisioned by User team.

iv. **SIEM Installation –** Vendor shall carry out the installation of the SIEM solution on 3-server cluster environment/ single node with cold standby server as per requirement and install the agents on all the hosts / VMs. The vendor shall ensure integration of the SIEM with Hosts, VMs, HCI infrastructure, LAN switches, Routers ,Firewall and syslog for detailed view of the events on the network. The SIEM implementation shall cover following reporting capability other than base feature of the products –

1) Failed login attempts
2) Failed authorization attempt
3) Detection of node or traffic other than approve network list
4) Detection of file system commands like rm
5) Network port scan attempt
6) Change in system binary

v. **Proxmox HCI VE Establishment -** Vendor needs to establish three Hyper- Converged Infrastructure (HCI) with Proxmox VE. Each infrastructure shall use 3 Nos of Config -1 Server. Following will be the strategy for deployment –

1) Each Server of a cluster will be deployed in different Rack to ensure cluster survives during a rack power failure
2) The 10G interfaces will be used for cluster heartbeat – as primary and secondary heartbeat channel connected on the core switch network
3) The 1G interface on the servers will be used as node interface.
4) The implementation of the Proxmox VE shall be as per OEM best practice guide. The VM resource allocation also shall be as per best performance recommendations.
5) NSIL/User shall provide the details of the physical host which needs to be migrated on the virtual environment. Vender needs to make detailed plan of the VMs and failover path within each cluster.
6) The success of the configuration and acceptance will be based on the verification of the configuration and after verification of the successful failure of the cluster nodes.
7) Vendor shall engage experienced engineers on the platform for implementation of the cluster.

vi. **Network Behavior Analytics (NBA/NBAD) Installation -** Vendor needs to install the NBA/NBAD collector for three segments of the network as described in the specification and has to ensure complete isolation of the segments via one way technology for data ingestion in NBA collector. Vendor has to ensure that NBA collector should not combine or join three segment of the network and bypass UTM/Firewall rules. However, for analysis purpose, all the logs can be combined and processed. Vendor shall ensure the NBA master controller node will be setup and a dash board will be setup to show the malicious activities detected. The vendor also needs to integrate the alerts in SIEM console. Vendor must ensure that only OEM part number is quoted for implementation support and must ensure yearly one visit by OEM engineer for at-least one weeks' time to tune all the policies and algorithms for better detection.

d. **Security Audit –** During the system implementation phase, vendor will be provided with security control implementation at location as per currently adopted standard. Vendor shall ensure all the security controls are implemented as per guideline and shall create required checklist and verification data after completion of the implementation. While making the implementation of any product, vendor must ensure the OEM recommended hardening standards are adopted for each implementation.

i. NSIL shall depute an expert team to verify the security implementation on the infrastructure and based on the satisfactory findings the implementation will be accepted.

ii. The function of the security implementation will be limited to the platform and capabilities which are delivered as per current contract and additional hardware or software will not be under the scope of implementation.

iii. Vendor shall also note that during onsite support activity, vendor must ensure the security implementation is maintained consistently. User shall conduct yearly security audit by internal expert team as per established standard. All the findings during verification will be with-in the vendor's scope of configuration delivery and shall be completed within one month of official notification.

25. Appendix 'Y' – UT Display Speifiation

A.0 UT & CDT Time Display

Device Type	:	NTP based UT and CDT Time coder with Display
1. Make & Model no. :		

A.1 Specifications

1. Display	:	Seven segment Nine digits display plus +/- segment
2. Time information	:	(a) Universal Time (UT) in Day:Hour:Minute:Second format (b) Count Down Time (CDT) in +/- Hour:Minute:Second format
3. Plus / Minus Sign	:	Off- during UT time information displaying and Plus (+) sign during CDT in counting UP and minus (-) sign during CDT time counting down
4. Input selection	:	Unit shall have Switch to select either UT input or CDT input or suitable provision to be done for displaying either UT or CDT time by reading input time information
5. NTP Over Ethernet	:	(a) Unit should display UT Time coming as Ethernet packets i.e. standard NTP Time output given by NavIC Receiver or GPS receiver (b) Unit should display CDT time coming as Ethernet packets (should support customized packets also) output by SHAR-ISRO CDT Time Format
6. Time Display	:	9 digit ultra-bright 4 inch height 7 segment display (format should be DOY:HH:MM:SS) representing Days (3 digits), Hours (2 digits), Minutes (2 digits) and Second (2 digits), preceded by alpha numeric sign display '+' for Count Up, '-' for Count Down and 'H' for Hold with clear gap (':'colon as separator) between Days, Hours, Minutes and Seconds or

			equivalent letter display 'up' for Count Up , 'dn' for Count Down and 'ho' for Hold.
	7. Time Display LED color	:	Bright Amber / Red colour
	8. Enclosure & Dimension	:	The unit shall be enclosed in a box. The unit dimensions shall be as per design with minimum bezel along the border of the seven segment displays
A.3	Connectivity		
	1. Connectivity	:	LAN – 2 ports / LAN-1port & IRIB-G port accordingly unit shall be designed for reading UT and CDT time
	2. Network capabilities	:	Yes, 10/100/1000 Ethernet Base-T RJ-45 connector
	3. EIA/IRIG-B input	:	IRIG-B modulated signal via BNC connector, level 500mV to 10Vpp suitable to output of NavIC / GPS receiver output
A.4	Power Supply	:	Built-in with power 230V +/- 10V AC 50-60Hz

26. Appendix 'Z' – Onsite Support

a. Resident Engineer / Onsite Support.

i. **Onsite Support Skill1:** Support for unified storage and backup software, Servers and hosts and VMs

ii. **Onsite Support Skill2:** Support for NMS, Network Switches, Routers and End node connectivity

iii. **Onsite Support Skill3:** Support for NGFW, SIEM, and Security Implementation in UTM and Security Compliance verification for network elements, server, hosts and VMs and NBA/NBAD

b. **Minimum Skillset Requirement –** The offered onsite resource shall have following minimum skillset requirement criteria –

i. Onsite Support Skill1:

1) Minimum 3 years onsite experience on offered Storage Product. Experience certificate to be attached.
2) Certification: Valid RHCSA (Redhat Certified System Administrator)

ii. Onsite Support Skill2:

1) Minimum 3 years onsite experience on offered Switching and Routing Products. Experience certificate to be attached.
2) Certification: Valid CCNA (Cisco Certified Networking Associate) Certificate

iii. Onsite Support Skill3:

1) Minimum 3 years onsite experience on offered NGFW or minimum two years' experience on offered SIEM Product. Experience certificate to be attached.
2) Certification: Certification on NGFW Advance Security Certification or Certification on any SIEM product

c. **Onsite Engagement –** The offered onsite Engineer shall have following engagements:

i. The resident engineers shall be positioned at Bhopal Control Center.

ii. The engineers shall have Weekly 6 days (8 AM to 5 PM) onsite engagement.

iii. Extended hours support during operational requirement or contingency

iv. Complimentary off for extended support based on mutual agreement of NSIL/User team

v. Yearly 15 days official leave will be granted on mutual agreement

vi. Leaves beyond allowed quota must be compensated with residential engineer of equivalent skill

vii. During release of onsite Engineer there must be three months notice period for knowledge transfer with new resource/onsite Engineer. The existing resource/ onsite Engineer have to ensure all the documents are updated and handed over to the new engineer.

d. **Roles and Deliverables:** The following are the roles and deliverables by the residential engineers –

i. The resident engineers shall be responsible for upkeep of the deployed systems in respective role which includes daily status check, configuration verification, firmware upgrade, fault and failure handling, logging calls with OEM and follow-up, providing logs for trouble-shooting, taking recovery action including fresh installation and replacement of hardware or software etc.

ii. Other than regular health check of the hardware and delivered configuration, the onsite support team shall ensure regular firmware update of the delivered hardware with a planned calendar of update schedule. The update activity will be carried out after due approval of the User/NSIL team. Vendor shall also ensure to implement the security configuration and settings as per existing configuration and also to ensure implementation of security guideline, as per OEM recommended guideline for newly migrated firmware version. During each firmware update cycle, vendor must make a fall back plan in case the upgrade is not complete within scheduled time.

iii. Though the roles are specific for engineers, based on requirement the residents' engineers may need to perform overlapping roles

iv. **Deliverables for Skill1:** Support for unified storage and backup software, Servers and hosts and VMs

1) Daily Verification
   - Status of Storage, Backup server, SAN switch, Tape Library, Servers, VMs, HCI interface and provide health check report on system health
   - Check the backup policy and report backup status
   - Check the status of file system at different servers (central storage and local servers) and report utilization
   - Check the logs of HCI and VMs and report anomalies

2) Weekly Verification
   - Overall report on system heath
   - Pending issues which are not closed last week
   - Update documentation on operation procedures
   - Test recovery of random files in alternate path from latest backups

3) Monthly Reporting
   - Consolidated reporting of the anomalies found and corrective action taken

- Report on parts/spare replacement and highlight pending issues
- Status of firmware or software upgrade (if action is identified)

v. **Deliverables for Skill2:** Support for NMS, Network Switches, Routers and End node connectivity

1) Daily Verification
   - Status of all the network devices in the network both in LAN and WAN (including remote), verification of the device logs and report anomalies
   - Check the status of NMS software , build new services views and alerts as required
   - Status on Port Security 802.1x on network
   - Check for KVM, RKM and Management network status
   - Check for status of data diode, interface and file flow
   - Check for status of Rsync, FTP and other file synchronization process
   - Check for all host connectivity including channel bonding
2) Weekly Verification
   - Configuration backup of all network device
   - Overall report on system heath
   - Link heath report indicating the error rates, downtime and bandwidth utilization
   - Pending issues which are not closed last week
   - Status of network security configuration and compliance report
   - Status of Host security controls as per standard provided
   - Update documentation on operation procedures
3) Monthly Reporting
   - Consolidated reporting of the anomalies found and corrective action taken
   - Report on parts/spare replacement and highlight pending issues
   - Status of firmware or software upgrade (if action is identified)

vi. **Deliverables for Skill3:** Support for NGFW, SIEM, and Security Implementation in UTM, NBA/NBAD and Security Compliance verification for network elements, server, hosts and VMs –

1) Daily Incident analysis, verification and reporting
2) Configuration of new rules
3) Adding new nodes and applications in log collector environment
4) Write parsers, connectors and other programs as necessary to enable integration of new devices with log aggregator
5) Building custom co-relation and notification rules
6) Verification of availability of all data point / collector status
7) Regular tuning of configuration of reduction of false positive notification

8) Whitelisting events and activates for exclusion

9) Configuration for automatic reporting and notification for customized report
10) Integration and monitoring of UTM. NBA/NBAD and antivirus logs
11) Configuration of new data points / collector interface
12) Upgradation and maintenance of log analysis software
13) Incident report preparation and submission as per User/NSIL provided template
14) Daily report –
    - No of open incidents
    - Action Pending from Sysadmin Team
    - Health Check report of all the hardware and software elements in SIEM, UTM fabric and Antivirus and Data Diode
    - Report generation as per NSIL/User provided template
15) Weekly Report–
    - Total No of incidents reported
    - No of open incidents
    - Total No of incidents closed
    - Status of signature update in UTMs and Desktop Antivirus
    - Change in security configuration or settings in Router, Switches, UTMs, Hosts and VMs.
    - Update documentation on operation procedures
16) Monthly Report –
    - Total No of incidents reported
    - No of open incidents
    - Total No of incidents closed
    - Threat categories of the incidents
    - Day wise breakup of incidents
    - Monthly Audit report as per provided Security Standard [This activity will be distributed across entire month and segment wise verification date to be recorded in the report]
    - Status of security patch update

e. **Monthly Review:** The vendor shall identify an account manager role who shall have online / onsite meeting with NSIL, User teamand site engineers on last week of every month to discuss the pending issues and review support deliverable status. The actions with in scope of the deliverables shall be identified and resolved by the vendor. Vendor shall deploy additional skills to ensure specialized maintenance activities is covered by additional temporary skillsets (subject matter experts) as required if any such action is identified during the review.

f. General terms:

i. Onsite (resident) support engineer is required for entire contract duration.

ii. Cost for each onsite skill to be quoted separately.

iii. Bio-data and two stamp size photographs of the Resident Engineer to be deployed shall be sent to the Focal Point for records. The Resident Engineer, once approved for the service, should not be changed by Service Provider, without the written concurrence from Focal point

iv. The resident engineer shall be responsible for carrying out all the routine health check, troubleshooting, co-ordination with different OEM in problem solving, firmware/software upgrades and updates storage system configuration changes etc and shall ensure service availability.

v. The resident engineer shall share the configuration and knowledge information with Bhopal and NSIL team periodically.

vi. Vendor shall ensure availability of resident engineer as per the details mentioned above.

vii. The engineer deployed shall reach the work spot well in time and strictly follow the rules and regulations regarding safety and security of NSIL.

viii. The engineer deployed is not authorized to communicate any official information they may come across during & after their working period, to any third party.

ix. Resident Engineer should be present during working hours. If the Service Provider fails to provide the same, Purchaser reserves the right to deduct a proportionate order value from the pending/future bills of the service provider for the period of absence.

x. If a resident Engineer proceeds on leave or leaves the Company, the replacement engineer to be deployed in advance so as to prevent any interruption in services rendered by them. I.e. new (replaced) resident Engineer should have been trained aprior, as an alternate. The same to be conveyed in advance to the Focal point, in writing.

xi. Purchaser reserves the right to seek replacement of the resident engineer if service is found not satisfactory.

xii. Purchaser reserves the right to reject any of the personnel deployed by the Service provider

xiii. The onsite engagement of the resident engineers shall start after completion of the implementation and site acceptance test of the setup.

xiv. The resident engineers must qualify the back ground verification criteria as set by User and NSIL for deployment on site.

xv. The resident engineers must abide by the physical and cyber security guideline as set by NSIL and User.

xvi. The vendor and all the onsite deployed engineers must sign NDA (non-disclosure agreement) with NSIL.

xvii. Except with the written consent of the Authority, the vendor shall not disclose

the contract or any provision, specification, plan, design, pattern, sample or information thereof to any third party.

27. Appendix 'AA' – Other Technical Terms and Conditions

a. **Common Terms and Conditions:** The following set of specifications shall be met by all the offered items unless explicitly specified.

i. Installation & System Support –

1) Vendor should install & commission all the systems as per the configuration at specified user site. The deployment configuration shall be provided during system installation phase.
2) The system implementation document for each element shall be provided by the vendor.
3) The installation shall include unpacking, integration, deployment of the delivered components and as per detailed scope as mentioned in technical specification.
4) Wherever required installation of operating system, upgradation of firmware/IOS, and installation of required device drivers & system libraries shall be carried out by the vendor.
5) Vendor should resolve all issues related to compatibility of hardware, drivers, and other system software with OS.
6) As part of User Acceptance Test (UAT), for all delivered items vendor needs to demonstrate the compliance to the tender specifications for each product. Vendor is required to make required test cases, record the test output and observation and complete the service migration for completion of UAT. Vendor shall provide installation and acceptance report as part of system installation on successful completion of system acceptance by end users.
7) Vendor shall provide required skilled man-power during system installation, service migration and acceptance at user site. The identified skilled man-power shall strictly follow the rules and regulations regarding safety and security of NSIL.
8) At the time of installation and commissioning of the configuration if it is found that some additional hardware accessories or software items with licenses are required to complete the configuration to meet the operational requirement of the configuration which were not included in the vendor's original list of deliverables then vendor is required to supply such items to ensure the completeness of the configuration at no extra cost. Vendor should ensure completeness of the list of deliverables in the offer to avoid such discovery during installation.

ii. **System Support –** Vendor shall provide on-call onsite support for the delivered set of systems during the warranty period. The support shall include onsite activities like failed component replacement, Operating system & device driver installation and configuration, firmware & IOS upgrade, troubleshooting and raising support call with OEM.

1) Vendor shall identify a support engineer in Palayamkottai & Delhi who shall provide on call basis onsite support requirements. The identified engineer shall

reach the work spot well in time and strictly follow the rules and regulations regarding safety and security as per User/NSIL requirement. Further equipment breakup for each location to be provided at the time of PO Placement.

b. Quality Requirements –

i. The design and production of critical subsystems like system motherboard, controllers etc., shall be under the control of manufacturer & international quality certified realization process.

ii. All subsystems of the system shall have been selected to achieve optimal performance and high reliability.

iii. The system architecture shall ensure maximum performance for data processing applications. The subsystems, the processor boards, the interconnections among subsystems and the software shall be properly matched to ensure maximum performance.

iv. Systems shall be only from a proven product line from highly reputed manufacturers. The product line shall be an internationally established brand reputed for high quality and with wide acceptance in deployment for mission critical and business critical functions in the industry.

v. The manufacturer of the system shall be in total control of the life cycle (Design, release, support, obsolescence and termination of the critical subsystems like motherboard, controllers etc.,) of the product.

c. Notes to the Vendor –

i. Vendor shall submit the following certifications from OEM on OEM's letter head for all deliverables except for SIEM tool, HCI Software, NMS Tool, Microsoft Windows, LAN Cables and Accessories, RHEL -

1) The vendor is authorized for participating in the bid
2) The offered hardware is not an obsolete product
3) The offered hardware / software components will not reach End of Support for atleast seven years from the date of supply
4) The offered hardware / software component is back to back supported by the OEM during the warranty period

ii. Vendor shall submit the following certifications from OEM on OEM's letter head, wherever applicable (Storage, Servers, Workstations, Laptops, All-in- One, NGFW, Router, Switch, NBA/NBAD etc). The OEM does not have any objection on retention of failed media (Hard disk or NVRAM) at Bhopal & Delhi during warranty replacements

iii. For all items in the list of deliverables offered by the vendor, the

manufacturer's part number should be clearly indicated. Offer of items without clear specification of part number is not acceptable.

iv. Vendor should indicate the part nos. of the deliverable items clearly. The part numbers & description of the items in the offer should match the part numbers & description of the items mentioned in the manufacturer's spec sheets.

v. The part numbers & description of the goods delivered should match the part numbers & description in the offer.

vi. Vendor should carefully consider all the clauses in the specifications and should ensure that their offer is complete in all respects at the time of submission. Complete technical documentation justifying the compliance should be enclosed along with their offer. Offer which are incomplete are liable to be considered noncompliant.

vii. Specifications of the major items have been provided in the enclosed document. In case any additional accessories/ software media/licenses are required to complete the configuration for full functionality and/or better manageability vendor should include such hardware accessories and related software elements or plug-ins with licenses in their offer.

viii. Systems from the manufacturers who primarily assemble systems by getting components/ subsystems from different suppliers and who do not have direct control over the production process/ quality of the items so obtained, will not be acceptable.

ix. Vendor should provide technical brochure from manufacturer for all subsystems to verify the current status (i.e. when released, whether due for replacement/obsolesce) the specification of the subsystems. The technical brochure shall give the details not only for the main system but also for all the subsystems and accessories. Technical brochure shall include details of

1) Functional specification.
2) Hardware & software configuration.
3) Configuration options.
4) Electrical & environmental specification.
5) Safety compliance details.
6) Physical dimension.
7) System test report and reliability metric

x. In case the approval of any Foreign Govt. agency, like US dept. of commerce, is required for the supply of any of the items, vendor should clearly indicate the items requiring such clearance. For such items vendor should obtain strong assurance from the manufacturer regarding their commitment to follow-up through the necessary clearance process. A written assurance to this effect should be enclosed with the technical offer.

d. Items for delivery at Delhi

i. List of Items to be transferred to Delhi from Bhopal after completion of UAT on user division request: -

1) Station Computers - 04 nos
2) Edge Switches - 04 nos
3) Routers - 02 nos
4) NGFW (Config-2) - 2 Nos

Post shipment, Vendor should support commissioning of these devices at Delhi

Annexure- II : Evaluation Process

(i) All the bidders who fulfil the minimum eligibility conditions of this EOI shall be further evaluated on the price quoted and the selection of partner will be done on L1 (Lowest bid) basis.

(ii) The evaluation shall be inclusive of quoted GST rates and bidder will be under obligation for quoting/charging correct rate of tax as prescribed under the respective Tax Laws. "GST rates as applicable, Vendor should furnish break up of GST rate" for items

(iii) The bidders are required to quote as per the BoQ attached in the tender and upload the same.

(iv) Blank or omitted items will be considered 'Nil' and treated as having Zero value. However, bidder is bound to provide all items as per the BoQ as per the terms and conditions of this EOI and NSIL, BANGALORE tender, without any extra cost to RailTel.

(v) In the annexure – I the bidders are requested to quote above/below/ at par for the percentages for each of the line item. The offer will be considered for all the line items put together as a whole and not as per the individual item wise.

(vi) Rates quoted against each schedule in above should be inclusive of basic rate, including GST, Freight, Insurance, all taxes and any other charges or cost quoted by the tenderer.

(vii) The engineer – in – charge can change i.e. add or delete or modify the location/ station/ Quantity/ materials as per the Railway requirement during the execution of the work. Detailed Technical specification are given in the Tender document.

(viii) The bidders are required to meet all eligibility criteria mentioned in this tender document and financial bids of eligible bidders will be opened.

(ix) Non- conformities between Figures and Words - If there is a discrepancy between words and figures, the amount in words shall be prevail.

(x) Priority, if any, for selection of partner will be provided as per RailTel's Business Associates policy and Agreed terms of Empanelment LOI/Agreement.

Annexure-III : Bid Security Declaration Form

(To be submitted on the Firm Letter Head)

Date:_____Tender No. _____

To,

RailTel Corporation of India Ltd.
No-6/1, 12th Main, Opp-Mount Carmel College,
Vasanthnagar, Bangalore 560052

Sub : SUPPLY, INSTALLATION, COMMISSIONING, OPERATION AND MAINTENANCE OF UPGRADATION OF IT INFRASTRUCTURE

I/We understand that, according to tender conditions, bids must be supported by a Bid Securing Declaration.

a) I/We accept that I/We may be disqualified from bidding for any contract with RailTel for a periodof three (3) year from the date of notification if I am/We are in a breach of any obligation under the bid conditions, made misleading or false representations in the forms, statements and attachmentssubmitted in proof of the qualification requirements;
b) If the bid is withdrawn or varied or modified in a manner not acceptable to theEmployer during the validity or extended validity period duly agreed by the Bidder.
c) Any effort by the Bidder to influence the Employer on bid evaluation, bid comparisonor contract award decision.
d) Fail to commence the work on the specified date as per LOA/Work order and/or. sign the Agreement AND / OR furnish the required Performance security.

I/We understand this Bid Securing Declaration shall cease to be valid if I am/we are not the successful Bidder, upon the earlier of (i) the receipt of your notification of the name of the successful Bidder; or (ii) thirty days after the expiration of the validity of my/our Bid.

Signed: (insert signature of person whose name and capacity are shown)

in the capacity of (insert legal capacity of person signing the Bid Securing Declaration)

Name: (insert complete name of person signing the Bid Securing Declaration)

Duly authorized to sign the bid for an on behalf of (insert complete name of Bidder)Dated on_day of_____(insert date of signing)

Corporate Seal (where appropriate)

Annexure IV: Format for COVERING LETTER

(To be submitted on the Firm's Letter Head)

EoI Reference No: Date:

To,

RailTel Corporation of India Ltd.
No-6/1, 12th Main, Opp-Mount Carmel College,
Vasanthnagar, Bangalore 560052

Sir/Madam,

Subject: UPGRADATION OF CCTV SYSTEM AND COMPREHENSIVE ANNUAL MAINTENANCE CONTRACT

Reference: Tender No: NSIL/RFP/IT/UPG/2025/01 DT: 12/11/2024

We, the undersigned bidder/s, having read and examined in detail all the bidding documents in respect to the RFP for procurement of firewall, do hereby propose to provide our services as specified in Tender.

Technical Response
We confirm having submitted the information as required by you in your Request for Proposal document. In case you require any other further information/documentary proof in this regard for evaluation of our bid, we agree to furnish the same in time to your satisfaction.

Deviations
We declare that all the services shall be performed strictly in accordance with the bid documents and there are no deviations from the requirements mentioned in this RFP

Performance Bank Guarantee
We hereby declare that in case the contract is awarded to us, we shall submit the contract performance bank guarantee in the form prescribed in the RFP.

Validity of this Bid
We agree to abide by this tender response for a period of 180 days after the date of opening of bids prescribed by the NSIL, BANGALORE and it shall remain binding upon us with full force and virtue, until, within this period, a formal contract is prepared and executed. This tender response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and DoT.

We undertake, if our proposal is accepted, to adhere to the implementation plan for the Proposed System at DoT put forward in RFP or such adjusted plan as may subsequently be mutually agreed between us and DoT or its appointed representatives.

We also hereby declare that information furnished in this Tender is true, complete and correct to the best of my knowledge and belief. I undertake that in the event of any information being found false or incorrect at any stage, my bid shall be liable to be cancelled/ terminated without any notice or compensation in lieu thereof along with any legal proceedings.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We understand that our bid is binding on us and that you are not bound to accept a Bid you receive.

It is hereby confirmed that I/We are entitled to act on behalf of our company/ corporation/ firm/ organization and empowered to sign this document as well as such other documents, which may be required in this connection.

We hereby submit EMD amount of Rs. _____ issued vide _____ from Bank _____.

Thanking you,
Yours faithfully

(Signature of the Authorized signatory)
Name :
Designation :
Phone No. :
Email id :
Date :

Authorized Signatory
Name & Designation

Annexure V : Format for Self-Certificate & Undertaking

Self-Certificate (To be on company letter head)

EoI Reference No: RailTel/SR/SBC/NSIL-CCTV/01 ; Dt. 10/07/2025

To,

RailTel Corporation of India Ltd.
No-6/1, 12th Main, Opp-Mount Carmel College,
Vasanthnagar, Bangalore 560052

Dear Sir,

Sub: Self Certificate for Tender, Technical & other compliances

1) Having examined the various Technical specifications in the EOI, we hereby confirm that we meet all specification.
2) We _____ agree to abide by all the technical, commercial & financial conditions of the NSIL, BANGALORE Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 pertaining to the portion against which the we have quoted in this EOI on back-to-back basis. We understand and agree that RailTel shall release the payment to selected partner after the receipt of corresponding payment from end client NSIL, BANGALORE 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 NSIL, BANGALORE Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 pertaining to the portion against which the bidder has quoted in this EOI on back-to-back basis.
4) We hereby agree to comply with all OEM technical & Financial documentation including MAF, Technical certificates/others as per end to end requirement mentioned in the NSIL, BANGALORE Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 pertaining to the portion against which the bidder has quoted in this EOI. We are hereby enclosing the arrangement of OEMs against each of the BOQ item quoted as mentioned NSIL, BANGALORE Tender No. NSIL/RFP/IT/UPG/2025/01 DT: 20/06/2025 pertaining to the portion against which the bidder has quoted in this EOI.
5) We hereby undertake to work with RailTel as per NSIL, BANGALORE tender terms and conditions. We confirm to submit all the supporting documents constituting/ in compliance with the Eligibility Criteria as required in the NSIL, BANGALORE terms and conditions like technical certificates, OEM compliance documents.

Authorized Signatory
Name & Designation

Annexure-VI: Details of the Bidder

Sl. No.	Particulars	Details
1.	Name of the Bidder	
2.	Address of the Bidder	
3.	Status of the Company (Public Ltd/ Pvt. Ltd)	
4.	Details of Incorporation of the Company	Date: Ref. #
5.	Details of Commencement of Business	Date: Ref. #
6.	Valid GST no.	
7.	Permanent Account Number (PAN)	
8.	Name & Designation of the contact person to whom all references shall be made regarding this tender	
9.	Telephone No. (with STD Code)	
10.	E-Mail of the contact person	
11.	Mobile No. of the contact person	
12.	Website	
13.	Financial Details (as per audited Balance Sheets) (in Cr)	

14.	Year	**2022-2023**	**2023-2024**	**2024-2025**
15.	Net Worth			
16.	Turn Over			
17.	PAT			

Authorized Signatory
Name & Designation

Annexure- VII :

(To be executed on Non-Judicial Stamp Paper of Rs.100/-)

FORMAT OF POWER OF ATTORNEY (in original)

In favour of signatory/s to the Tender, duly authenticated by Notary Public.

POWER OF ATTORNEY IN FAVOUR OF ---------- (Name, Designation, Company name)

TO ALL TO WHOM THESE PRESENTS shall come, I, (Name & address of the authorized person to sub-delegate/delegate powers, delegated on him by the Board of Directors) do hereby sub-delegate/delegate, in terms of the powers delegated to me by the Board of Directors, ----------
-(name of the Co.) to Shri (name, designation & address of the Attorney) the following:

NOW KNOW YE AND THOSE PRESENTS that I, (Name & address of the authorized person to sub-delegate/delegate powers, delegated on him by the Board of Directors), do herebyauthorize and empower Shri ---------- (name, designation & address of the Attorney) to do severally amongst others, for the purpose of carrying on our business, the following:

a) To represent lawfully the (name of the Co.) for obtaining bid/tenderdocuments, prepare, sign, execute and submit tenders for execution of "SUPPLY, INSTALLATION, COMMISSIONING, OPERATION AND MAINTENANCE OF UPGRADATION OF IT INFRASTRUCTURE

b) To discuss the technical and financial matters, negotiate and accept prices andtake decisions regarding terms and conditions and sign agreements and contracts and also to bind the (name of the Co.) to the arbitration clause included in thecontract.

c) For all or any of the purposes here of to sign and deliver or otherwise execute such deed or deeds, transfer or transfers, endorsement or endorsements and toperform such other acts, matters, things as the Attorney shall consider requisiteor advisable as full and effectively as the Company could do, if present and acting there.

I, (Name & address of the authorized person to sub-delegate/delegate powers, delegated on him by the Board of Directors) in terms of the powers delegated to me by the Board of Directors of (name of the Co.), do hereby agree that all acts, deeds and things done by the said Attorney by virtue of this power of attorney, shall be construed asacts, deeds and things done by the Company.

I, (Name & address of the authorized person to sub-delegate/delegate powers, delegated on him by the Board of Directors), further undertake to ratify and confirm whatever our said attorney shall do or cause to be done for the Company, the said Company, in the premises, by virtue of the powers hereby given.

WHEREAS, this sub-delegation is signed and delivered to Shri ---------- (name & designation of the Attorney), on this_____day of_____, 20 (Twothousand_____).

WHEREAS, even though this sub-delegation is signed on this_____day of _____20_____(Two thousand_____), will have effect from the date he signs and receives this delegation.

IN WITNESS WHEREOF, I, (Name & address of the authorized person to sub- delegate/delegate powers, delegated on him by the Board of Directors) has, this _____ day of_____20_____ (Two thousand_____) set my hands and subscribed my signature unto this instrument.

SIGNED AND DELIVERED ON

_____BY

(Name of authorized person to delegate powers)

WITNESS:

SIGNED AND RECEIVED ON

_____BY

(Name & designation of Attorney)

Annexure - VIII
Turnover Details

TO WHOMSOEVER IT MAY CONCERN

This is to certify that the annual turnover furnished by << COMPANY NAME >> for last 5 years .....

Financial year	Total Turnover, Net worth, Profit & Loss Statement of the Company (Rs.)
2019-20	
2020-21	
2021-22	
2022-23	
2023-24	

This is as per the Statement of Accounts which has been duly verified by me and found correct.

Place:

Date:

Seal & Signature of
Chartered Accountant

Annexure- IX : Format for Undertaking on Litigation(s)

(To be submitted in firm/ company letter head)

This is to certify that << COMPANY NAME >> is not involved in any litigation that may have an impact of affecting or compromising the delivery of services as required under this RFP.

We also hereby declare that information furnished in this Tender is true, complete and correct to the best of my knowledge and belief. I undertake that in the event of any information being found false or incorrect at any stage, my bid shall be liable to be cancelled/ terminated without any notice or compensation in lieu thereof along with any legal proceedings against.

Thanking you,
Yours faithfully

(Signature of the Authorized signatory)

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

CONFIDENTIAL AND MUTUAL NON- DISCLOSURE AGREEMENT

THIS AGREEMENT MADE ON THIS_____DAY OF _____, 2020 AT

BETWEEN

_____a company incorporated in India under the provisions of the Companies Act, 1956 and having its Registered Office at (Hereinafter referred to as "Company") represented by its Managing Director / CEO Mr./Ms _____duly authorized for the same which expression shall unless repugnant to the meaning or context thereof be deemed to mean and include, its Directors, affiliates, successors and permitted assigns of the **FIRST PART**

AND

RailTel Corporation of India Limited, is a Government of India undertaking under the Ministry of Railways duly incorporated under the provisions of the Companies Act, 1956 and having its registered office and Corporate office at Plat-A, 6th Floor, Office Block Tower-2, East Kidwai Nagar, New Delhi- 110023 (hereinafter referred to as "RailTel") , represented by Dy. General Manager/Law & CS Mr. J.S. Marwah duly authorized for the same which expression shall mean and include unless repugnant to the context, its successors, representative and permitted assigns of the **SECOND PART**

WHEREAS

A. Company is poised to provide _____ services to _____ for _____ project.

B. RAILTEL is a Public Sector Undertaking (PSU under the Ministry of Railways), setup interalia to exploit Indian Railway's large telecom infrastructure.

C. COMPANY and RAILTEL are working-out/ negotiating a possible commercial and strategic business relationship (hereinafter Purpose).

D. During the course of the above negotiations RAILTEL and COMPANY (including their affiliates may in conjunction with the purpose and for their mutual benefit, disclose to each other certain information being proprietary and/or of confidential nature, and/or RAILTEL and COMPANY may receive and share or be grant access by the other to such confidential and/or proprietary information which is considered trade secret, proprietary, confidential and/ or sensitive.

E. The parties and its affiliates wish to ensure the protection and secrecy of their respective confidential information which may be disclosed, received or granted access to by the other party and wish to reduce to writing, their agreement in this respect.

NOW THEREFORE in consideration of the mutual promises, covenants and representations recorded herein by the parties hereto and such additional promises and understanding as are hereinafter set forth, the parties agree as follows:

1) Definition

For the purpose of this agreement, the term 'Confidential Information' shall mean and include any information or data of a scientific, technical, commercial or financial nature disclosed by the Disclosing party to the Receiving Party or which is obtained by a party from the other whether in writing, pictorially, in machine readable form, on disc, mail or orally, or by any other means/ modes of disclosure and including without limitation any information contained in any written or printed document, hardware, firmware and software, information related to technology and business activities (including, but not limited to, communication systems, telecommunication, business outlooks, revenue, pricing, trade secrets), computer programs, software (including, without limitations, code, software output, screen displays, file hierarchies and user interfaces), formulas, data, inventions, techniques, technology, know-how, processes, ideas, (whether patentable or not), schematics, specifications, drawings, product designs, product plants, programming, services, strategies, third party confidential information, and corporate and personnel statistics, customer lists (potential or actual) and other customer-related information, supplier information, sales statistics, market intelligence, marketing, business working, operations, parent, subsidiaries, affiliates and other business strategies and other commercial information of a confidential nature.

(a) The party disclosing the Confidential Information is referred herein to as "Disclosing Party" and the party to which such Confidential Information is disclosed is referred to herein as "Recipient Party".

(b)"Affiliate" of the Party shall mean the Company or other person who or which is either controlled by the respective Party or who controls the respective Party or who or which is controlled by same person/ entity who controls the respective Party, either by way of significant shareholding, voting rights or technical collaboration whether directly or indirectly through its affiliate.

2) Neither party shall be required to disclose any particular information (including but not limited to Confidential Information) to the other and disclosure of any such information shall be entirely voluntary and at the sole discretion of the parties and to the extent deemed necessary by it and is not intended to, and shall not, create any contractual or other relationship or obligation of any kind beyond the terms of this Agreement nor any provision or disclosure of information (including but not limited to Confidential Information) as contemplated hereunder, shall be construed as creating, conveying, transferring by one party on the other any rights, license or authority in or to the information provided. The parties hereto shall use the Confidential Information only for the limited purpose of exploring/ finalizing the possible business relationship between the parties hereto and for no other purpose whatsoever.

3) Both the parties acknowledge and understand that any exchange of confidential Information of any nature shall not commit or bind the other to enter into a contract or otherwise and that neither party shall rely on any information provided by the other as a commitment or an inducement to act or not to act in any given manner. Further neither party shall be liable

to the other in any manner whatsoever for any decisions, obligation, costs or expenses incurred, changes in business practices, plans, organization, products, services or otherwise of the other, as a result of this Agreement or any exchange of Confidential Information hereunder.

4) Both the Parties agrees and undertake to regard and preserve as Confidential Information provided by each to the other or which may be disclosed, received or granted access to by either party or come to the knowledge of either party in any manner in connection with the negotiations for the possible business relationship.

5) (a) In maintaining the Confidential Information hereunder both parties agree that they shall not, without first obtaining the written consent of the other, disclose or make available to any person, firm or enterprise, reproduce or transmit, or use (directly or indirectly) for its own benefit or the benefit of others, any Confidential Information save and except that either party may disclose any Confidential Information to its Directors, officers, employees, or advisors on a "need to know" basis to enable them to evaluate such "Confidential Information" in connection with the negotiation for the possible business relationship between the Parties hereto.

(b) Both parties shall ensure that the said employee(s) and / or the said person(s) shall maintain confidentiality with regard to the disclosed Confidential Information, if any, and shall issue two suitable instructions and/or get two suitable written undertakings or agreements executed to binds its employees and/or the said person(s) to the same obligations of confidence and safeguarding as the parties hereto and to adhere to the confidentiality/ non-disclosure terms contained in this Agreement.

(c) Save and except for the purposes mentioned in clause (a) above both parties further agree that neither party will part with/ disclose any "Confidential Information" received by it to any other person directly or indirectly nor make copy(s) or reproduce in any way (including without limitation store in any computer or electronic system any written material/ documents containing "Confidential Information" and such written material/ documents will be retained under strict confidentiality by the receiving party.

(d) Both parties further agree that the confidential information which may pertain to or touch upon any regulatory aspects and/or dealings of either party with any statutory / government/ related agencies/ bodies, whether the said information is received verbally or in writing, will not be disclosed in any manner, either directly or indirectly, to any other persons except to its Directors, employees or advisors on a strictly 'need to know' basis.

(e) 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 unauthorised disclosure, but in no event shall a less than reasonable degree of care be exercised by either party.

6) It is mutually acknowledged and agreed that information shall not be considered "Confidential Information" to the extent, that such information : (a) at the time of disclosure was in the public domain or (b) is already known to the receiving party free of any confidentiality obligation at the time it is obtained from other party; or (c) after disclosure is or becomes publicly known or available through no wrongful act of the receiving party; or (d) is rightfully received from a third party without restriction or (e) is

approved for release, disclosure, dissemination or use by written authorization from the Disclosing Party; or (f) is required to be disclosed pursuant to a requirement of a governmental agency or law so long as the parties provide each other with timely prior written notice of such requirement and provide all reasonable co-operation in regard to taking protective action against such disclosure requirement; or (g) is disclosed after expiry of 5 (five) years from the date of expiry or earlier termination of this agreement.

However, before any party discloses any Confidential Information under clause 6, either party (to the extent permitted by law) uses its best endeavour to:

(a) Inform other party of any circumstances and the information that will be disclosed

(b) Give the other party a copy of a legal opinion indicating that disclosure is necessary

(c) consult with the other party as to possible steps including without limitation, protective orders, or other appropriate remedy to avoid or limit disclosure and take those steps where they would not result in significant adverse consequences to the other party and

(d) Gain assurances as to the confidentiality from the body to whom the information is to be disclosed.

If either party is unable to inform the other party before confidential information is disclosed, it will (to the extent permitted by law) inform the other party of the full circumstances of the disclosure and information that has been disclosed immediately after disclosure.

7) Both parties further agree and undertake not to disclose the information marked "Confidential Information" of the other to their agents or contractors without prior written approval from the other and without having first obtained from each agent or contractor a separate written agreement or undertaking binding them to the same obligations of confidence and safeguarding.

8) The parties further recognize that it may be necessary or appropriate for COMPANY to disclose Confidential Information to other Group Companies not named herein. For this purpose, COMPANY guarantees the observance and proper performance of other Group Company to whom Confidential Information is disclosed as above, of the terms and conditions of this agreement.

9) Both parties further agree to indemnify and keep indemnified each other against all actual loss and damage which the Disclosing Party may suffer because of any breach of this agreement by the Recipient Party of the Confidential Information. Always provided that

a. the Disclosing Party shall forthwith give written notice to the recipient Party of the loss and damage; and
b. the Recipient Party shall be furnished with satisfactory documentary evidence of such actual loss and damage.

10) Both parties further agree that upon termination/ expiry of this Agreement or at any time during its currency, at the request of the Disclosing Party the Recipient Party shall promptly

(and in any case, within 15 days of request), deliver to the Disclosing Party all copies of the Confidential Information in its possession or under its direct or indirect control or shall destroy all memoranda, notes and other writings prepared by the recipient party or its affiliates, Directors, officers, employee s or advisors to the extent the same are based on the confidential information with a written statement to the effect that upon such return the Receiving Party has not knowingly retained in its possession or under its control, either directly or indirectly, any Information or copies of such (other than Confidential Information embedded in the Receiving Party's records).

The confidentiality obligations set out herein above shall survive any such return or destruction of Information. Further The provisions set out herein above shall not apply to copies of electronically exchanged Information made as a matter of routine information technology backup and to Information or copies thereof which must be stored by the receiving Party, its Affiliates or its advisers according to provisions of mandatory law, provided that such Information or copies thereof shall be subject to an indefinite confidentiality obligation according to the terms and conditions set forth herein.

11) Both parties acknowledge that the confidential information coming to the knowledge of the other may relate to and/or have implications regarding the future strategies, plans, business activities, methods, processes and or information of the parties which afford them certain competitive and strategic advantage. Accordingly neither party will use the confidential information or strategies, plans, business activities, methods, process, information, and /or competitive and strategic advantage to the other.

12. Each party understands that the other party may currently or in the future be developing information internally, or receiving information from third parties that may be similar to the "confidential Information" Accordingly, nothing in this agreement will be c construed as a representation or inference that either party will not develop products, or have products developed for it, or enter into joint ventures, alliances, or licensing arrangements that, without violation of this agreement, compete with the products or systems embodying the "confidential Information".

13. Except as specifically provided herein, disclosure of confidential information by either party pursuant hereto shall not be deemed to grant to the Recipient party, any rights, interest or property in such confidential information and accordingly both parties agree that they will not directly or indirectly claim or submit any application for grant of any patent, copyright, design right or other intellectual property Rights in, to or on the basis of the confidential information.

14. The parties hereto acknowledge and agree that in the event of a breach or threatened breach by the other of the provisions of this Agreement, the party not in breach will have no adequate remedy in money or damages and accordingly notwithstanding anything contained in clause 18 hereof, the party not in breach shall be entitled to injunctive relief against such breach or threatened breach by the party in breach : provided , however, no specification in this confidentiality Agreement of a specific legal or equitable remedy shall be construed as a waiver or prohibition of any other legal or remedies in the event of a breach or threatened breach of this Agreement and the remedies specified herein shall be in addition to all other reliefs and remedies available to the parties under prevailing laws.

15. No failure or delay be either party in exercising or enforcing any right, remedy or power hereunder shall operate as a waiver thereof, nor shall any single or partial exercise or enforcement of any right, remedy or power preclude any further exercise or enforcement of any right, remedy or power preclude any single or partial exercise or enforcement thereof or the exercise or enforcement of any of any other right, remedy or power.

16. Each Party acknowledges that the other Party makes no representation or warranty as to the accuracy or completeness of any of the Information furnished by or on its behalf. Only those representations and warranties which are made in a final definitive agreement relating to the purpose of the disclosure of the Information will have legal effect.

Each party represents and warrants to the other that it is a corporation duly organised and validly existing in the jurisdiction of its incorporation. Each party represents that it has full corporate power and authority to enter into this Agreement and to do all things necessary for the performance of this Agreement. The Disclosing Party warrants that the Confidential Information has not been provided in breach of any other agreements having legal binding of any nature with the third party(s).

Unless documented and agreed otherwise in respect of any individual disclosure of Confidential Information, each party warrants that it will use its best endeavours to ensure that any Confidential Information it discloses or it intends to disclose to the other party under the provisions of this agreement is complete and accurate but PROVIDED ALWAYS that the disclosing party has exercised such best endeavours:

The parties acknowledge that:

(a) such Confidential Information as is disclosed by the Disclosing party under this Agreement is accepted by the Receiving Party it at its own risk; and
(b) it releases the Disclosing party from all claims, actions, and suits in relation to such Confidential Information (including its use under this Agreement).

17. This agreement will be governed by the laws of India and jurisdiction shall be exclusively vested in the courts at New Delhi, India only.

18. If any matter arises between the parties about this agreement, then the parties shall meet to discuss the matter and shall negotiate in good faith to endeavour to resolve the matter arising the matter, however.

a. If any matter arising has not been resolved by the parties within thirty (30) days after the date the party raising the matter gave notice of it to the other party: then

b. the matter shall be submitted by either party to Arbitration. Arbitration shall be held in New Delhi, India. The arbitration shall be conducted as per the provisions of Indian Arbitration and Conciliation Act 1996 and any statutory modification or re-enactment thereof.

c. Each party to the dispute shall appoint one Arbitrator each and the two Arbitrators shall appoint the third or the presiding Arbitrator. The arbitration proceedings shall be conducted in the English language. The courts of law at New Delhi, India alone shall have the jurisdiction. The arbitration award shall be final and binding upon the parties and judgement may be entered thereon, upon the application of either party to a court having jurisdiction.

d. Each party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the parties unless the award otherwise provides.

19. This agreement shall not be assignable or transferable by either party without the written consent of the other party.

20. No license to a Party hereto, under any trademark, patent, copyright or any other intellectual property right, is either granted or implied by the conveying of Information to such party.

21. This agreement shall remain valid for a period of 3 (three) years from the date of execution of this Agreement which term may be extended by mutual consent in writing of both the parties. This agreement may be terminated by either party by giving 30 (thirty) days' notices in writing to the other party without assigning any reason whatsoever. However, the obligations of each party hereunder shall survive the termination or earlier determination or expiry of this Agreement and shall continue and be binding upon the parties irrespective of whether the discussion between the parties materialize into a specific understanding/business relationship or not for a further period of 5 (five) years after termination / expiry of the agreement.

22. All notices required by this Agreement shall be in writing, and shall be personally delivered, sent by registered post or by commercial courier, addressed as follows:

To Company: Mr/Ms _____

To RAILTEL:
Attn: Mr. J. S. Marwah
RailTel Corporation of India Limited, Plat-A, 6th Floor,
Office Block Tower-2, East Kidwai Nagar, New Delhi- 110023

Nothing in this provision shall be construed to prohibit communication by more expedient means, such as by telephone or facsimile transmission, to accomplish timely communication. However, to constitute effective notice, written confirmation of a telephone conversation or an original of

facsimile transmission must be sent by registered post, by commercial carrier, or hand-delivered. Each party may change the address by written notice in accordance with this paragraph. Notices delivered personally shall be deemed communicated as of actual receipt; mailed notices shall be deemed communicated as of four days after mailing, unless such date is a date on which there is no mail service. In that event communication is deemed to occur on the next mail service day.

23. This agreement supersedes all prior discussions and writings with respect to the confidential information and constitutes the entire Agreement between the parties with respect to the subject matter hereof and no modifications of this Agreement or waiver of the terms and conditions hereof shall be binging upon either of the parties hereto, unless

approved in writing by an authorizes representative of each party. In the event that any of the provisions of this Agreement shall be held by court or other Tribunal of competent jurisdiction to be unenforceable, the remaining portions hereof shall remain in full force and effect and this Agreement shall be interpreted and construed accordingly.

24. This Agreement is executed in duplicate, each of which shall be deemed to be the original and both when sent together shall be deemed to form one and single document.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the date and year written above.

For RailTel Corporation of India Ltd.

Sign:	Sign:
Name:	Name:
Title:	Title:

Annexure – XI PROFORMA FOR SIGNING THE INTEGRITY PACT
(On Stamp Paper of Rs.100/-)

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

And ……., here in after referred to as "The Bidder/ Contractor"

Preamble.

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

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

Section 1- Commitments of the Principal

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

No employee of the principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

The principal will during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the process or the contract execution.

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

2. If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

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

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

The Bidder(s)/contractor(s) will not, directly or through any other persons or firm, offer promise or give to any of the Principal's employees involved in the tender process or the execution of the

contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage during tender process or during the execution of the contract.

The Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

The Bidder(s)/Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s) /Contractors will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the bidder(s)/contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative should be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers' as annexed.

The Bidder(s)/Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

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

Section 3: Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings". Copy of the "Guidelines on Banning of business dealings" is annexed.

Section 4: Compensation for Damages

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

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

Section 5: Previous Transgression

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

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

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

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

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

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

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

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

Section 8: Independent External Monitor / Monitors

1. The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

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

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

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

5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action, or tolerate action.

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

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

8. If the Monitor has reported to the CMD, RailTel, a substantiated suspicion of an offence under relevant IPC/PC Act, and the CMD, RailTel has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

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

Section 9: Pact Duration

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

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

Section 10: Other Provisions

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

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

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

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

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

	(Office Seal)
Place ————————	
Date ————————	
Witness 1: (Name & Address)	
	———————————————— ———————————————— ————————————————
Witness 2: (Name & Address)	
	———————————————— ———————————————— ————————————————

Annexure-XII: Past Performance details

Sl.No	Description	Details by the tenderer	Remarks, If any
1	Name of the Work		
2	Value of the work		
3	Letter of Award No and Date		
4	Original Period of completion		
5	Extended period of completion		
6	Portion of work of IT Network Infrastructure		
7	No of geographically dispersed locations in which work has been done for		
8	No of cities/ towns covered with the network under the above work		

It is certified that the IT Network Infrastructure under the above work has been done in federated.

Annexure- XIII : Undertaking for End of Support

Date:

To
RAILTEL CORPORATION OF INDIA LIMITED
No-6/1, 12th Main,
Opp-Mount Carmel College,
Vasanthnagar, Bangalore 560 052

Subject: End of Support Letter

Reference: Tender Number –

Madam/Sir,

We <OEM> ensure that the devices quoted <Device Name and Model> for the above referenced tender will not be declared end of Support for a period of 5 years from the date of Supply.

Thanking You

For < OEM>
< (Authorized Signatory)>

Annexure- XIV -

UNDERTAKING ON INDEMNIFICATION

We_____(Bidders Name) hereby agree and undertake to indemnify, keep indemnifies, depended and hold harmless the RailTel & NSIL and its Officers against all losses, penalties, costs and expenses, duties of any kind whatsoever which mayarise on account of breach un-authorized act, fraud deed or any other acts of ours or anyof our personnel. We hereby further agree and undertake to indemnify and keepindemnifies against any order passed by any executive, quasi-judicial or judicial authoritywherein the Railtel & NSIL is compelled to obey the order which arise due to breach of contract by us.

We_____(Bidders name) shall indemnify, protect and defend at ourown cost, New Mangalore Port Authority and its agents & employees from & against any/all actions, claims, losses or damages arising out of;

i. Any violation in course of execution of the contract of any legal provisions or any right of third parties.
ii. Failure to exercise the skill and care required for satisfactory execution of the contract.
iii. Shall indemnify NSIL against all claims for compensation by or on behalf of any workman employed by us in connection with the contract, for injury or death by accident under the Workman Compensation Act (Act VIII of 1923) as amended from time to time.

We_____(Bidders name) shall be responsible for all commissionsand omissions on part of manpower engaged for the purpose. NSIL shall not be responsible in any manner whatsoever, in matters of injury/death/health etc. of our employees performing duties under the contract.

We_____(Bidders name) hereby undertake that ,

a. The workforce deployed under this contract will be provided with all the necessary safety gears and equipment for the job.
b. Bidder/deployed staffs will follow all the required safety procedures while executing the job.

Sign and Seal of the Bidder/ Bidders Authorized representative

Annexure- XV -

Financial Bid Format

Name of Work: Supply, Installation, Commissioning, Operation and Maintenance of IT Infrastructure

Contract No:

Name of the Bidder/ Bidding Firm / Company :	

PRICE SCHEDULE

(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevent columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)

NUMBER #	TEXT #	NUMBER #	TEXT #	NUMBER #	NUMBER	TEXT	NUMBER #	NUMBER #	TEXT #
Sl. No.	Item Description	Quantity	Units	BASIC RATE In Figures To be entered by the Bidder Rs. P	GST Charges (in %)	Technical Spec / Requirement (As per Document B)	TOTAL AMOUNT Without Taxes in Rs. P	TOTAL AMOUNT With Taxes	TOTAL AMOUNT In Words
1	2	4	5	13	17	18	53	54	55
1	Workstation	54	Nos			Appendix 'A'	0.00	0.00	INR Zero Only
2	Monitor	74	Nos			Appendix 'B'	0.00	0.00	INR Zero Only

3	**NAS Storage (250 TB)**	**1**	**Nos**			**Appendix 'C'**	**0.00**	**0.00**	INR Zero Only
4	**Tape Backup**	**1**	**Nos**			**Appendix 'C'**	**0.00**	**0.00**	INR Zero Only
5	**Server (Rack) - Config-1**	**24**	**Nos**			**Appendix 'D'**	**0.00**	**0.00**	INR Zero Only
6	**Edge Switch**	**32**	**Nos**			**Appendix 'E'**	**0.00**	**0.00**	INR Zero Only
7	**Core Switch**	**2**	**Nos**			**Appendix 'F'**	**0.00**	**0.00**	INR Zero Only
8.1	**UTM / NGFW - Config-1**	**2**	**Nos**			**Appendix 'G'**	**0.00**	**0.00**	INR Zero Only
8.2	**UTM / NGFW - Config-2**	**6**	**Nos**			**Appendix 'G'**	**0.00**	**0.00**	INR Zero Only
8.3	**UTM Hardware Authentication Token**	**20**	**Nos**			**Appendix 'G'**	**0.00**	**0.00**	INR Zero Only
9	**NGFW Logger & Traffic Analyser**	**1**	**Nos**			**Appendix 'G'**	**0.00**	**0.00**	INR Zero Only

10	**NGFW Manager**	**1**	**Nos**			**Appendix 'G'**	**0.00**	**0.00**	INR Zero Only
11	**End Point Protection & Managemen t Tool**	**150**	**Nos**			**Appendix 'G'**	**0.00**	**0.00**	INR Zero Only
12	**Interconnec t Router - Config-1**	**2**	**Nos**			**Appendix 'H'**	**0.00**	**0.00**	INR Zero Only
13	**Interconnec t Router - Config-2**	**4**	**Nos**			**Appendix 'H'**	**0.00**	**0.00**	INR Zero Only
14	**Server Room Structured Cabling and Accessories**	**1**	**Nos**			**Appendix 'I'**	**0.00**	**0.00**	INR Zero Only
15	**All-in-one PC**	**6**	**Nos**			**Appendix 'J'**	**0.00**	**0.00**	INR Zero Only
16	**NMS Laptop**	**2**	**Nos**			**Appendix 'K'**	**0.00**	**0.00**	INR Zero Only
17	**ATS Device**	**8**	**Nos**			**Appendix 'L'**	**0.00**	**0.00**	INR Zero Only
18	**STC Server Node**	**8**	**Nos**			**Appendix 'M'**	**0.00**	**0.00**	INR Zero Only

19	**MCP Server**	**6**	**Nos**			**Appendix 'N'**	**0.00**	**0.00**	INR Zero Only
20	**Thin Client AIO**	**14**	**Nos**			**Appendix 'M' and 'N'**	**0.00**	**0.00**	INR Zero Only
21	**LCD Display with Trolley / Wall mount (75 inch)**	**3**	**Nos**			**Appendix 'O'**	**0.00**	**0.00**	INR Zero Only
22	**Syslog Servers - Config-2**	**5**	**Nos**			**Appendix 'P'**	**0.00**	**0.00**	INR Zero Only
23	**SIEM Server/ Security Analytics Server - Config-3**	**3**	**Nos**			**Appendix 'Q'**	**0.00**	**0.00**	INR Zero Only
24	**Printer - Color**	**2**	**Nos**			**Appendix 'R'**	**0.00**	**0.00**	INR Zero Only
25	**Printer - BW**	**8**	**Nos**			**Appendix 'S'**	**0.00**	**0.00**	INR Zero Only
26	**NMS Software with Lics**	**1**	**Nos**			**Appendix 'T'**	**0.00**	**0.00**	INR Zero Only
27	**RKM**	**8**	**Nos**			**Appendix 'U'**	**0.00**	**0.00**	INR Zero Only

28.1	**KVM (40 Port) - Config-1**	**1**	**Nos**			**Appendix 'U'**	**0.00**	**0.00**	INR Zero Only
28.2	**KVM (8 Port) - Config-2**	**2**	**Nos**			**Appendix 'U'**	**0.00**	**0.00**	INR Zero Only
29	**SIEM Software with 3500 EPS**	**1**	**Lot**			**Appendix 'V'**	**0.00**	**0.00**	INR Zero Only
30	**Network Behavior Analytics (NBA/NBAD)**	**1**	**Lot**			**Appendix 'W'**	**0.00**	**0.00**	INR Zero Only
31	**One Time Implementation + Documentation**	**1**	**Lot**			**Appendix 'X'**	**0.00**	**0.00**	INR Zero Only
32	**Onsite Support - 2 Skills for 5 years**	**5**	**years**			**Appendix 'Z'**	**0.00**	**0.00**	INR Zero Only
33	**Onsite Support - Security Service - 1 Skill for 5 years**	**5**	**years**			**Appendix 'Z'**	**0.00**	**0.00**	INR Zero Only
34	**UT Display**	**24**	**Nos**			**Appendix 'Y'**	**0.00**	**0.00**	INR Zero Only
35	**Windows Server OS 2022**	**6**	**Nos**				**0.00**	**0.00**	INR Zero Only

36	**CAMC charges per year including charges for onsite support- 2 skills and Onsite support - security service - 1 skill**	**2**	**years**			**As per RFP**	**0.00**	**0.00**	INR Zero Only
Total in Figures							**0.00**	**0.00**	INR Zero Only
Quoted Rate in Words		**INR Zero Only**							

Note:

Above rates are inclusive of packing, forwarding, freight, insurance, commissioning, warranty or any other charges.

The total cost column will be used for evaluation of the tender for determining the L1 cost.

Annexure-XVI(AFFIDAVIT)

FORMAT FOR AFFIDAVIT TO BE SUBMITTED BY TENDERER ALONG WITH THE TENDER DOCUMENTS

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

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

1. I/we the tenderer (s), am/are signing this document after carefully reading the contents.
2. I/we the tenderer(s) also accept all the conditions of the tender and have signed all the pages in confirmation thereof.
3. I/we hereby declare that I/we have downloaded the tender documents from RailTel website www.railtelindia.com / https://railtel.enivida.com. I/we have verified the content of the document from the website and there is no addition, no deletion or no alternation to be content of the tender document. In case of any discrepancy noticed at any stage i.e. evaluation of tenders, 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 tender 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 tenders, it shall lead to forfeiture of the tender EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the tenderer)** _____ 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 SD and Performance guarantee besides any other action provided in the contract including banning of business for five years on entire RailTel.

DEPONENT
SEAL AND SIGNATURE OF THE TENDERER

VERIFICATION
I/we above named tender 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 SIGNATURE
OF THE TENDERER

Place:
Date:

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

न्यूस्पेस इंडिया लिमिटेड (एनसिल)
NewSpace India Ltd. (NSIL)
(अंतरिक्ष विभाग के अधीन भारत सरकार की एक कम्पनी)
(A Central Public Sector Enterprise under Department of Space)

EXECUTIVE SUMMARY

RFP for upgradation of IT infrastructure including its Supply, Installation, Commissioning, Operation and Maintenance of IT Infrastructure

NewSpace India Limited (NSIL), a wholly owned Government of India company under Department of Space (DOS), is the commercial arm of Indian Space Research Organization (ISRO).

NSIL through this RFP aims to select vendor for Supply, Installation, Commission, operation and maintenance of upgradation of IT Infrastructure. The overall scope of work of the project includes establishment of dedicated IT infrastructure as per the scope of this tender at Bhopal and Delhi. Other sites may also be included.

The objective of the present RFP is to seek proposals from bidders for Supply, Installation, Commissioning, Operation and Maintenance of upgradation of IT Infrastructure.

Work packages and Deliverables under the RFP:

List of deliverables/ items / service required to be delivered as part of the scope of the detailed RFP is as follows:-

Ser	Description	Qty
1	Workstation	54
2	Monitor	74
3	NAS Storage (250 TB)	1
4	Tape Backup	1
5	Server (Rack) - Config-1	24
6	Edge Switch	32
7	Core Switch	2
8	UTM/NGFW-Config-1	2

	UTM/ NGFW - Config-2	6
	UTM Hardware Authentication Token	20
9	NGFW Logger & Traffic Analyser	1
10	NGFW Manager	1
11	End Point Protection & Management Tool	150
12	Interconnect Router - Config-1	2
13	Interconnect Router - Config-2	4
14	Server Room Structured Cabling and Accessories	1
15	All-in-one PC	6
16	NMS Laptop	2
17	ATS Device	8
18	STC Server Node	8
19	MCP Server	6
20	Thin Client AIO	14
21	LCD Display with Trolley / Wall mount (75 inch)	3
22	Syslog Servers - Config-2	5
23	SIEM Server/ Security Analytics Server - Config-3	3
24	Printer - Color	2
25	Printer - BW	8
26	NMS Software with Lics	1
27	RKM	8
28	KVM (40 Port) - Config-1	1
	KVM (8 Port) - Config-2	2
29	SIEM Software with 3500 EPS	1 lot
30	Network Behavior Analytics (NBA/NBAD)	1 lot
31	One Time Implementation + Documentation	1 lot
32	Onsite Support - 2 Skills for 5 years	5 years
33	Onsite Support - Security Service – 1 Skill for 5 years	5 years
34	UT Display	24

35	Windows Server OS 2022	6
36	Service migration of existing LDAP/NIS, Storage, NGFW, Routers, Switches, Syslog, Storage, Management interfaces, workstation, VMs etc. to the new hardware/platform.	Further details are in detailed RFP.
37	CAMC charges per year including onsite support- 2 skills and Onsite support – security service – 1 skill	2

The table above “List of Deliverables” (not exhaustive), list “include major deliverables for Upgradation of IT Infrastructure system, but are not limited to,”. Bidder to note that the offer needs to include all the items required to realize the IT Infrastructure as per the required configuration and specification in the detailed RFP.

Delivery schedule:

32 weeks for operationalization including delivery, installation, commissioning, and migration of required services from date of acceptance of PO/Contract.

Bidder Eligibility Criteria:

1. The bidder shall be System Integrator (SI) / OEM / any Authorized Agent/Vendor for OEM/SI or an organization/ a limited company, private company or any agency capable of taking up works of such nature and magnitude on a turnkey basis and shall produce an undertaking from respective major OEMs that the bidder is an authorized entity to quote for this tender and will provide support and spares directly to purchaser, if required, for the offered system (major items) and also that the offered system (major items) will be supported by the respective major OEMs for the period of minimum 7 years (5 years warranty and 2 years CAMC) after commissioning (go-live as defined in the tender).

1. Bidder shall provide details of financial profile of the company, product range, manpower profile, turn-over status and experience in the field of setting up IT Infrastructure along with its techno-commercial bid.

2. The bidder must submit all documents listed in this document.

3. The bidder must have minimum annual sales turnover of least Rs.12 crores for at least three of last five financial years. The copies of relevant documents or a certificate from a Chartered Accountant certifying the turnover amounts should be submitted along with the bid.

4. The bidder must have must have installed and commissioned IT infrastructure project for at-least one of the options as mentioned below (in the last three years as on the date of floating of the RFP):

   Option 1:
   - One similar work at ₹24 crore or more (including GST)

   Option 2:
   - Two similar completed works each costing at ₹15 crore or more (including GST)

   Option 3:
   - Three similar completed works each costing at least ₹12 crore each or more (including GST)

   The copy of purchase order and installation certificates signed by the End user clearly stating that the bidder has carried out installation of the said system to this effect must be submitted with the bid document. (Any prototype installation / test set-up or installation in bidder's or its affiliate premises will not be accepted).

5. The bidder must quote for all the items given in the scope of the RFP. Partial order placement is not possible except as per the clauses mentioned in this tender document.

General Terms & Conditions for Tender:

2. This is a **two-part public tender**. Bidder shall submit its offer in two parts viz., Techno-commercial bid and financial bid in the manner as mentioned in the detailed RFP. If price information is revealed (either in part or full) in the techno-commercial bid, total bid is liable for rejection.

3. All information supplied by the Bidders as part of their bids in response to this RFP, may be treated as contractually binding on the Bidders, on successful award of the assignment by NSIL based on this RFP.

4. Bidder shall submit Non-Disclosure Agreement duly signed by Authorized Signatory as per the format provided by NSIL.

5. Bidder is required to provide EMD of INR 75,00,000.0 (Seventy Five Lakh rupees only) shall be made through Bank Guarantee in favor of "NewSpace India Limited", towards bidder participation for the tender.

6. The cost of the RFP document is Rs. 29,500/- (Twenty Nine Thousand Five Hundred rupees only including GST). **After making payment for the tender document and signing NDA ONLY the detailed RFP document will be provided to bidder. Bank Details for paying RFP documents cost are:**

   Account Name: NewSpace India Limited
   Bank A/C No: 38345843981

IFSC Code: SBIN0009042

7. Bidder shall submit an undertaking, duly signed by authorized signatory, while submitting the bid, stating that there has been or is no outstanding bankruptcy/ insolvency, judgment or pending legal action that could impair operations of the bidder.

8. Bidder shall submit Make in India declaration in line with Government Public Procurement (Preference to Make in India), Order 2017, P-45021/2/2017-PP (BE-II) dated 16.09.2020 and subsequent clarification No P-45021/102/2019-BE-II-Part (1) (E-50310) dated 04.03.2021.

9. Bidder shall submit declaration In-line with Department of Expenditure's (DoE) Public Procurement Division Order vide ref. F.No.6/18/2019-PPD dated 23.07.2020 & 24.7.2020 regarding restrictions under Rule 144 (XI) of the General Financial Rules (GFRs), 2017.

NSIL Purchase Department Contact No:

Tel: (080) 2322 7777 Ext. 137, E-mail: purchase@nsilindia.co.in

REQUEST FOR PROPOSAL

RFP No NSIL/RFP/IT/UPG/2025/01

DOCUMENT A
(COMMERCIAL DOCUMENT)

Supply, Installation, Commissioning, Operation and Maintenance of
Upgradation of IT Infrastructure

NewSpace India Limited (NSIL)
A Govt. of India company under Department of Space, Govt. of India
Brigade Rubix, Watch Factory Road, Yeshwanthpur
Bangalore – 560013, INDIA

Contents

Section-1: RFP and Instructions to bidders

1. Introduction

NewSpace India Limited (NSIL), a wholly owned Government of India company under Department of Space (DOS), is the commercial arm of Indian Space Research Organization (ISRO). NSIL as part of its mandate to commercially explore the products and services emanating from Indian Space Programme, is keen to harness the potential of indigenously developed ISRO technology and provide space-based solutions to meet various requirements including the requirements from Govt. and strategic sector related to telecommunication, broadcasting, broadband services, security etc.

NSIL through this RFP aims to select vendor for Supply, Installation, Commission, operation and maintenance of upgradation of IT Infrastructure. This activity is part of a user project.

The overall scope of work of the project includes establishment of dedicated IT infrastructure as per the scope of this tender at two different user sites at Bhopal (major site) and Delhi. Other sites may also be included.

The objective of the present RFP is to seek proposals from bidders for Supply, Installation, Commissioning, Operation and Maintenance of upgradation of IT Infrastructure.

This Request for Proposal is for "Supply, Installation, Commissioning, Operations and Maintenance of upgradation of IT Infrastructure" as per the specifications described in this document.

2. Instruction to bidders

NSIL, hereby invites through this Public Tender for upgradation of IT Infrastructure. Interested Vendors (viz. our Registered Vendors) shall visit the URL i.e. https://etenders.gov.in/eprocure/app for downloading of tender documents, bid preparation, hash submission, bid submission etc. The Tenders shall be duly digitally signed and encrypted by the Tenderers using their class -3 Digital Signature Certificate with encryption.

The bids in response to this tender is to be submitted electronically in place of offers in 'Hard Copy under Sealed Envelope' as is being done conventionally. Tender Submission, Tender Closing and Opening activities will be done electronically and online. No oral, email, telephone, telegraphic tenders or tenders submitted in hard copies/physical form will be entertained.

Techno-commercial bid shall cover all technical information and compliance statement, deliverables and delivery schedule and commercial terms and conditions – except pricing details. In case of any price information revealed (either in part or full) in the techno-commercial bid, total bid will get rejected.

The RFP consists of two documents (This document and Document B: Separate document for technical details). This document consists of three sections as per following:

Section-1: RFP and Instruction to Bidders

Section-2: Terms and conditions of RFP

Section-3: Annexures and BG Format

2.1. General Instructions

A. While every effort has been made to provide comprehensive and accurate background information, requirements and technical details, Bidders must form their own conclusions about the solution(s) needed to meet the requirements of this RFP.

B. All information supplied by the Bidders as part of their bids in response to this RFP, may be treated as contractually binding on the Bidders, on successful award of the assignment by NSIL based on this RFP.

C. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written Purchase Order has been executed by NSIL. Any notification of preferred bidder status by NSIL shall not give rise to any enforceable rights by the Bidder. NSIL may cancel this RFP at any time prior to a formal written Purchase Order being executed by the authority.

D. The bidders are advised to study all instructions, forms, terms, requirements, and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications. Any incomplete bid in any form is liable for rejection.

E. The Authorized Signatory of the Bidder shall initial all relevant pages of the Technical and the Financial Bids.

F. The Bidder shall issue a statement undertaking total responsibility for delivery of the components, subsystem, systems and services described in the Document B – Technical Document of this RFP.

G. Communication details:

Name of the Contact Point:	Dy. Manager, Commercial, NSIL
Postal address for sending the Bids / seeking Clarifications:	NewSpace India Limited (NSIL) 11th Floor, Brigade Rubix, 20, Watch Factory Road, Yeshwanthpur Bangalore 560013.
Contact Details:	Tel: (080) 2322 7777 Ext. 137 E-mail: Commercial Queries: purchase@nsilindia.co.in Technical Queries: it@nsilindia.co.in

H. The bid should be prepared and submitted by the Eligible Bidders in English language only.

I. Schedule of the Bidding Process is as follows:

Document Reference No	NSIL/RFP/IT/UPG/ 2025/01
RFP issue Date	As per CPPP
Pre-bid meeting	
Last date for seeking clarifications	
Last date for bid submission	

J. NSIL shall not be responsible for any non-receipt/ non-delivery of the documents due to technical snag whatsoever at Bidder's end.

K. Bid received after due date will not be considered for further evaluation. The bids submitted by fax / e-mail etc. shall not be considered. No correspondence will be entertained on this matter.

L. Bidder shall submit Make in India declaration in line with Government Public Procurement (Preference to Make in India), Order 2017, P-45021/2/2017-PP (BE-II) dated 16.09.2020 and subsequent clarification No P-45021/102/2019-BE-II-Part (1) (E-50310) dated 04.03.2021. Additional certifications as per relevant MII orders to be provided by the bidder.

M. NSIL reserves the right to reject in full or part, any or all bids without assigning any reason thereof. NSIL reserves the right to assess the Bidder's capabilities and capacity. The decision of the NSIL shall be final and binding in this regard.

N. Bid should be free of over writing. All erasures, correction or addition must be clearly written attested by the Authorized Signatory.

O. If, in the price structure quoted for the required deliverables / services, there is discrepancy between the unit price and total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail and the total price corrected accordingly.

P. If there is an error in a total corresponding to the addition or subtraction of subtotals in the financial bid, the subtotals shall prevail, and the total shall be corrected.

Q. **Validity of bid:** Bid shall remain valid for a period of 180 days from the bid submission date.

R. A pre-bid meeting will be arranged within two weeks of publication of this RFP. The pre-bid meeting will be held on virtual mode and the interested bidders are required to inform the details of the participants vide email to "purchase@nsilindia.co.in". The details of the meeting will be informed subsequently.

2.2. Vendor / bidder Eligibility Criteria:

A. The bidder shall be System Integrator (SI) / OEM / any Authorized Agent/Vendor for OEM/SI or an organization/ a limited company, private company or any agency capable of taking up works of such nature and magnitude on a turnkey basis and shall produce an undertaking from OEM that the bidder is an authorized entity to quote for this tender and will provide support and spares directly to purchaser, if required, for the offered system (major items) and also that the offered system (major items) will be supported by the OEM for the period of minimum 7 years after commissioning (go-live as defined in the tender).

B. Bidder shall provide details of financial profile of the company, product range, manpower profile, turn-over status and experience in the field of setting up IT Infrastructure along with its techno-commercial bid.

C. The bidder must submit all documents listed in this document.

D. The bidder must have minimum annual sales turnover of at least Rs.12 crores for at least three of last five financial years. The copies of relevant documents or a certificate from a Chartered Accountant certifying the turnover amounts should be submitted along with the bid.

E. The bidder must have must have installed and commissioned IT infrastructure project for at-least one of the options as mentioned below (in the last three years as on the date of floating of the RFP):

Option 1:
- One similar work at ₹24 crore or more (including GST)

Option 2:
- Two similar completed works each costing at ₹15 crore or more (including GST)

Option 3:
- Three similar completed works each costing at least ₹12 crore each or more (including GST)

The copy of purchase order and installation certificates signed by the End user clearly stating that the bidder has carried out installation of the said system to this effect must be submitted with the bid document. (Any prototype installation / test set-up or installation in bidder's or its affiliate premises will not be accepted).

F. The bidder must quote for all the items given in the scope of the RFP. Partial order placement is not possible except as per the clauses mentioned in this tender document.

G. Bidder is required to provide EMD of INR 75,00,000.0 (Seventy Five Lakh rupees only) shall be made through Bank Guarantee in favor of "NewSpace India Limited", towards bidder participation for the tender.

2.3. Withdrawal or / and Modification of Bid by bidder:

1. An Eligible Bidder may withdraw its Bid (technical and/ or financial) by writing to the address indicated for bid submission in the schedule of the bidding process prior to final bid submission date indicated in the schedule of the bidding process.
2. Request for withdrawal of a bids post the bid submission deadline shall normally not be considered, however in case a Bidder still wishes to withdraw a bid post the bid submission deadline, this may lead to disqualification of the Bidder. In addition to this, NSIL reserves right to give the Bidder a tender holiday for specified period decided by NSIL.
3. Bids withdrawn shall not be opened and processed further.

2.4. Bid document cost

The cost of the RFP document is Rs. 29,500/- (Twenty-Nine Thousand Five Hundred rupees only including GST). **After making payment for the tender document and signing NDA ONLY the detailed RFP document will be provided to bidder.**

2.5. Documents required along with Techno-commercial bid:

Sr. No.	Document Requirement	Documentary evidence
1	Payment of Bid document cost	Demand draft along with techno-commercial bid
2	Signed and Stamped Copy of the Bid Documents	Bid Document which is duly signed and stamped by the Authorized Signatory of the bidder.
3	Bidder Profile	A brief profile of the organization, its audited balance sheet for last 3 years, copy of annual tax returns for last 3 years, GST and PAN number, company URL, registered office address and contact information for the authorized person responsible for this project.
4	Work Experience	Bidder shall submit relevant documentary proof as required in the tender document.
5	Legal Status of the Bidder The Bidder shall be registered in India under Companies Act, 1956 or as amended. The Bidder shall be in continuous operation in India for a period of at least 5 years as on the date of the issue of RFP.	The Bidder shall submit • Copy of company Registration certificate • Copy of PAN card • Copy of GST registration
6	Non-Disclosure Agreement	The Bidder shall submit Non-Disclosure Agreement as per the format indicated in Annexure-G (Section-3) of this RFP signed by Authorized Signatory.
7	Track Record if bidder	An undertaking shall be submitted, duly signed by authorized signatory, stating that there has been or is no outstanding bankruptcy, judgment or pending legal action that could impair operations of the bidder.
8	Integrity Pact	An undertaking shall be submitted, duly signed by authorized signatory, for the Integrity Pact as mentioned in Annexure-F (Section-3) of this RFP.
9	Documents as per checklist- B	All documents as per Annexure B (Section-3).

2.6. Financial bid requirements:

1. The Bidder must submit the Financial Bid to indicate the price as per template provided in BOQ (*.xls) format. The Bidders shall quote prices in INR only. In case of any pricing information not covered in given template, bidder can provide the same in separate table in financial bid.
2. The Bidders shall quote for the entire scope of contract on a "overall responsibility" basis such that the total bid price covers all obligations of the Eligible Bidders, mentioned in or to be reasonably inferred from the bidding documents in respect of providing the product/services, including transportation of system/ hardware to Authority designated site locations.
3. The Bidders shall give the required details of all applicable taxes, duties, other levies and charges including transportation costs, etc. in respect of direct transaction between the Authority and the Eligible Bidder in the financial Bid.
4. No price escalation by the bidders shall be permitted during the contract period. The bidders are advised to quote a firm price that shall be valid for the entire duration of the contract.
5. The CAMC cost quoted for each year separately should not be less than 5% of the total supply cost (without GST).

2.7. Tender Submission:

1. It is a Two-Part Bid.
2. The interested Bidders may fill up the details in the application forms attached as Annexures – A to H and other documents requested in Document B – Technical document of this tender.
3. Proposal NOT submitted as per the specified format will be out-rightly rejected.
4. **The interested bidders may submit their Proposal online (https://etenders.gov.in/eprocure/app) on or before the deadline for submission of tender.**
5. Any Proposal received by NSIL after the prescribed deadline for submission of Proposal will be summarily rejected. NSIL shall not be responsible for any kind of delay or non-receipt / non-delivery of the documents.
6. Any deviation from the Tender specifications & terms and conditions will not be accepted.
7. After the completion of the selection process, the selected Bidder will be informed.
8. The Bidder should submit the filled-up Tender applications forms (Annexures – A to H) along with necessary documents electronically in .pdf format.
9. Commercial Bids of only Technically qualified bidder will be opened for further evaluation.

2.8. Bid Evaluation Criteria:

Total Bid evaluation process will take place as per following sequence:

1. First will be opening of Techno-commercial bid for bids received before due date in prescribed format. The venue, date and time for opening the Techno-commercial bid will be indicated through emails.
2. The Bids received by the NSIL shall be opened with advance intimation to bidders. Bidder can see the details once technical bids are open, on E-tender portal.

3. Techno-commercial evaluation of all the opened bids by NSIL.
4. NSIL may constitute a Tender Evaluation Committee (TEC) to evaluate the Techno-commercial bid of the Bidder. NSIL / Tender Evaluation Committee (TEC) shall evaluate the responses to the RFP and all supporting documents / documentary evidence. Inability to submit requisite supporting documents/documentary evidence by Eligible Bidder may lead to rejection of their bids.
5. During technical evaluation process if NSIL / TEC feels some clarification required from the bidder in order to fully evaluate his bid, the same will be communicated to respective bidder by e-mail/portal. In that case bidder shall provide his reply within stipulated time provided by NSIL in the e-mail/portal.
6. NSIL / TEC shall examine the bids to determine whether they are complete, whether the documents have been properly signed and whether the bids are generally in order. Any bids found to be nonresponsive for any reason or not meeting any criteria specified in the RFP, shall be rejected by NSIL / TEC and shall not be included for further consideration.
7. After successful completion of technical evaluation, all technically qualified bids will be selected for price / financial bid opening. The date and time for opening of the Financial Bid shall be communicated to the Technically qualified Bidder through email/portal.
8. The bids received from the Technically Qualified Bidders shall be ranked in ascending order of the quote (Financial Bid) as per the requirements and quantity mentioned in the RFP.
9. The technically qualified bidder quoting the Lowest (Lumpsum) Quote for the project shall be deemed the "Selected Party" (L1 Bidder). For the purpose of arriving at the lowest price (L1), quotes inclusive of applicable taxes and levies etc. will be considered.
10. For the purpose of identifying L1 vendor for awarding contract under this RFP, the total price quoted for all the items/services including total cost of 5 years warranty and 2 years CAMC along with the applicable taxes will form the basis of comparison between the eligible bidders.

2.9. Amendment of the RFP

1. At any time prior to the due date for submission of bid, NSIL may, for any reason, whether at its own initiative or in response to a clarification requested by prospective Eligible Bidder(s), modify the RFP document by amendments. Such amendments shall be published in NSIL Website/portal, in the form of corrigendum and shall form an integral part of RFP document. The relevant clauses of the RFP document shall be treated as amended accordingly.
2. It shall be the responsibility of the prospective Eligible Bidder(s) to check from time to time for any amendment in the RFP document in NSIL's website/portal. In case of failure to get the amendments, if any, NSIL shall not be held responsible.
3. In order to allow prospective Eligible Bidders a reasonable time to take the amendment into account in preparing their bids, NSIL, at its discretion, may extend the deadline for submission of bids. Such extensions shall be communicated to the Eligible Bidders via update in NSIL's website/portal in the form of corrigendum.

2.10. Right to vary quantity/ Tolerance Clause

To take care of any change in the requirement, the Authority reserves the right to 25% plus/minus increase or decrease the quantity of the required goods up to that limit without any change in the terms & conditions and prices quoted by the Seller. While awarding the contract, the quantity ordered can be increased or decreased by the authority.

2.11. Confidentiality:

All the material / information shared with the Bidder during the course of this procurement process as well as the subsequent resulting engagement following this process with the Bidder, shall be treated as confidential and should not be disclosed in any manner to any unauthorized person under any circumstances. The employees of the Bidder who are proposed to be deployed on the project at specified sites need to furnish a Non-Disclosure Agreement (NDA). The Bidder shall execute and maintain all copies of the Non-Disclosure Agreement (NDA) and shall produce it when sought by NSIL.

2.12. Awarding of Contract and its execution:

1. NSIL will notify the Selected Party (ies) in writing by e-mail/portal, regarding the contract award/ Purchase Order. In this case party (ies) shall confirm the order acceptance in writing to NSIL within 10 days of receipt of contract from NSIL.
2. In case of non-receipt of the acceptance of the contract by NSIL, it will be treated as "accepted" by the vendor.
3. For every supply order issued under Frame work Contract, the party shall submit at his own expense unconditional and irrevocable Security deposit (SD) cum Performance Bank Guarantee (PBG) valued at 3% of the Supply Order to NSIL. This SD / PBG shall be submitted within 15 days of reception of supply order from NSIL with a total validity period for 8 years.
4. The PBG shall be from a Nationalized Bank or a Scheduled Commercial Bank in the format prescribed in Annexure-C of this RFP, payable on demand, for the due performance and fulfilment of the supply order by the party.
5. In case the project is delayed beyond the intended schedule, the performance bank guarantee shall be accordingly be extended by the party till completion of scope of work as mentioned in the section-2 of this RFP.
6. The SD / PBG may be discharged/returned by NSIL upon being satisfied that there has been due performance of the obligations of the bidder under the contract. However, no interest shall be payable on the performance bank guarantee.

Section-2: Terms & Conditions of the RFP

1. General Terms and Conditions

A. Upon technical evaluation the vendor would be required to give a detailed presentation to the committee for the compliance of the entire configuration quoted, along with the necessary benchmarks. The vendor needs to provide the ATP documents, which are mutually agreed upon.

B. The Vendor shall provide a detailed technical compliance statement for offered products and specifications. The compliance matrix shall also cover all terms and conditions mentioned in the tender (Document A and Document B).

C. The Vendor must take full responsibility for total supply, installation, integration, migration, interoperability, compatibility and successful testing of all the quoted items.

D. The Vendor shall ensure compatibility of the components used in the solution.

E. The Vendor shall list bill of materials for all the items and sub items offered along with part numbers in the techno commercial bid.

F. The total solution document shall be provided by the Vendor along with the techno commercial bid.

G. The quoted make and models must be clearly specified for all items/ sub-items. Full technical specifications and literature must be provided for all the quoted items including sub-items to substantiate the compliance.

H. Complete ownership of ensuring the solution in a working condition as per the requirements mentioned in the RFP lies with the tenderer. Any components/accessories like cables, etc. shall be included in the response and Tenderer agrees to supply the items missed/short shipped at no additional cost.

I. The Vendor (System Integrator) must be authorized partner of OEMs and shall provide authorization certificate from the OEM for this tender. The Vendor shall submit the entire Manufacturer Authorisation Form (MAF) certificate from the OEM.

J. Near obsolete and out-dated technology based products shall not be quoted/offered as a part of the solution.

K. The source of all items shall be either from our country or from the countries who have a good heritage on cyber security and amicable to our country.

L. Each item offered shall have a minimum support life of seven years. Certificate to this effect to be produced from the respective OEM that the product delivered under this RFP/tender will be provided back-to-back OEM support for 7 years post-go-live (go live as defined in the tender). OEM shall not deny renewal of back-to-back support for 7 years lifespan post-go-live of the items delivered under the scope of this RFP.

M. The Vendor must have certified skilled, trained and experienced manpower with technical competence for all the quoted products.

N. Certification of the skilled manpower and their police verification on every new induction to be provided to the NSIL/end-user.

O. Any required software/drivers to make the given items usable shall be delivered along with media and documentation.

P. All standard and optional items, if any, must be clearly indicated.

Q. All the licenses for given hardware and software shall be perpetual. Licensing information for software must be provided in detail wherever applicable.

R. As part of warranty and post warranty, CAMC support, the Vendor shall ensure availability of spares at least for the next seven years after installation and successful integration of the equipment.

S. Installation, integration and support to be performed/provided at Bhopal site (major site) and New Delhi site. If required, installation may be carried out at other sites as specified by the authority at no additional cost.

T. Vendor should do system tuning for better performance of overall system and OEM would be responsible for tuning components.

U. Mutually acceptable acceptance test procedure (ATP) document shall be provided by the Vendor. Acceptance Test on the supplied equipment must be conducted as per the ATP document.

V. Supplied items shall work on 220V, 50 Hz, AC power supply.

W. The vendor should bring out any gaps in the RFP, which may be required for the total solution and quote for total solution at no additional cost.

X. Any defective/failed storage hard disk or magnetic media (LTO) or any storage media shall be replaced by the Vendor without insisting on return of defective media. The defective media will not be given to the Vendor.

Y. Vendor shall treat all the batteries supplied along with server's/storage systems as components and shall replace batteries during warranty period/ CAMC without extra cost.

Z. The quoted product should be in strict conformance with the declaration in Annexure - H: Land Border Sharing Declaration.

AA. Complete ownership of ensuring the solution in a working condition as per NSIL requirements mentioned in the RFP lies with the vendor. Any components/accessories like cables, etc. shall be included in the response and Vendor agrees to supply the items missed/short shipped at no additional cost.

BB. Any accessory/hardware/software not explicitly executed from the scope of work, but required to ensure the proper functioning of the hardware/software as per the scope of the tender shall be deemed to implicitly included in the tender and has to be provided by the vendor without any additional cost.

2. Liquidated Damages.

In the event of the Seller's failure to submit the Bonds, Guarantees and Documents except in cases of exemptions, supply the stores/goods and conduct trials, installation of equipment, training, etc as specified in this contract, the Buyer may, at his discretion, withhold any payment until the completion of the contract. The BUYER may also deduct from the SELLER as agreed, liquidated damages to the sum of 0.5% of the contract price of the delayed/undelivered stores/services mentioned above for every week of delay or part of a week, subject to the maximum value of the Liquidated Damages being not higher than 10% of the value of delayed stores.

3. Risk & Cost Purchase clause.

A. Should the stores or any instalment thereof not be delivered within the time or times specified in the contract documents, or if defective delivery is made in respect of the

stores or any instalment thereof, the Buyer shall after granting the Seller 45 days to cure the breach, be at liberty, without prejudice to the right to recover liquidated damages as a remedy for breach of contract, to declare the contract as cancelled either wholly or to the extent of such default.

B. Should the stores or any instalment thereof not perform in accordance with the specifications / parameters provided by the SELLER during the check proof tests to be done in the BUYER's country, the BUYER shall be at liberty, without prejudice to any other remedies for breach of contract, to cancel the contract wholly or to the extent of such default.

C. In case of a material breach that was not remedied within 45 days, the BUYER shall, having given the right of first refusal to the SELLER be at liberty to purchase, manufacture, or procure from any other source as he thinks fit, other stores of the same or similar description to make good: -
    a. Such default.
    b. In the event of the contract being wholly determined the balance of the stores remaining to be delivered thereunder.

D. Any excess of the purchase price, cost of manufacturer, or value of any stores procured from any other supplier as the case may be, over the contract price appropriate to such default or balance shall be recoverable from the SELLER. Such recoveries shall not exceed 10% of the value of the contract."

4. Termination of Contract.

The Buyer shall have the right to terminate this Contract in part or in full in any of the following cases: -

A. The delivery of the material is delayed for causes not attributable to Force Majeure for more than three months after the scheduled date of delivery.

B. The Seller is declared bankrupt or becomes insolvent.

C. The delivery of material is delayed due to causes of Force Majeure by more than six months provided Force Majeure clause is included in contract.

D. The Buyer has noticed that the Seller has utilised the services of any Indian/Foreign agent in getting this contract and paid any commission to such individual/company etc.

E. As per decision of the Arbitration Tribunal.

5. Payment Terms & Schedule

The Successful bidder will be paid at different milestones of the project appropriately. The details of the payment are as follows:

No	Time Line	Milestone	Payment value
1.	T0	Placing of order	
2.	T0 + 45 Days	Advance Payment	15% of Contract value minus the charge for training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC (Against 110% Advance Bank Gurantee). If advance payment is not claimed, the payment for this milestone will be released at the time of acceptance of delivery at both sites i.e. along with completion of milestone 3 and 4.
3.	T0 + 16 Weeks	Delivery & BOM verification* of Hardware & Software at Bhopal	30% of Contract value minus the charge for training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC
4.	T0 + 18 Weeks	Delivery & BOM verification* of Hardware & Software at New Delhi	30% of Contract value minus the charge for training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC
5.	T0 + 24 Weeks	Installation & Commissioning – phase1 [Firewall, Switches, Routers, NMS (upto n/w map), Storage, Back-up S/W, Filesystem migration]	7% of Contract value minus the charge for training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC
6.	T0 + 28 Weeks	Installation & Commissioning – phase 2 [All HCI environments, migration of FTP, rsync services, NIS/LDAP, data diode interfaces, syslog migrations, SIEM configuration, NBA/NBAD, Antivirus installation]	7% of Contract value minus the charge for training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC
7.	T1=T0 + 32 Weeks	Installation & Commissioning – phase 3 [Remaining services including ATP as per the scope of the RFP and Go-Live]	6% of Contract value minus the charge for training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC
8.	T1 + 2 Weeks	Completion of Training	Training cost -1st year
9.	T1 + 1 Year	Successful Warranty Support for 1st Year	1% of Contract value minus the charge for training, manpower

			(onsite support- 2 skills & onsite support - security service 1 skill) and CAMC + manpower cost (onsite support- 2 skills & onsite support - security service 1 skill)
10.	T1 + 2 Year	Completion of Training	Training cost -2nd year
11.	T1 + 2 Year	Successful Warranty Support for 2nd Year	1% of Contract value minus the charge for training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC + manpower cost (onsite support- 2 skills & onsite support - security service 1 skill)
12.	T1 + 3 Year	Completion of Training	Training cost -3rd year
13.	T1 + 3 Year	Successful Warranty Support for 3rd Year	1% of Contract value minus the charge training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC + manpower cost (onsite support- 2 skills & onsite support - security service 1 skill)
14.	T1 + 4 Year	Completion of Training	Training cost -4th year
15.	T1 + 4 Year	Warranty Support for 4th Year	1% of Contract value minus the charge for training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC + manpower cost (onsite support- 2 skills & onsite support - security service 1 skill)
16.	T1 + 5 Year	Completion of Training	Training cost -5th year
17.	T1 + 5 Year	Warranty Support for 5th Year	1% of Contract value minus the charge for training, manpower (onsite support- 2 skills & onsite support - security service 1 skill) and CAMC + manpower cost (onsite support- 2 skills & onsite support - security service 1 skill)
18.	T1 + 6 Year	Completion of Training	Training cost -6th year
19.	T1 + 6 Year	CAMC Support for 6th Year	CAMC Support for 6th Year
20.	T1 + 7 Year	Completion of Training	Training cost -7th year
21.	T1 + 7 Year	CAMC Support for 7th Year	CAMC Support for 7th Year

*BOM Verification: BOM verification involves only quantity and part no verification of the received items as per PO.

Note 1: In case migration of a service/component cannot be completed due to unavailability of Software/ any other input to be provided by NSIL side, and the said component is not being procured within the scope of this RFP, the installation and commissioning would be deemed to be completed subject to the condition that all the remaining terms and conditions are complied and duly fulfilled as per the requirements and scope of this RFP.

Note 2: Relevant penalty clauses/ SLA will be applicable as defined in the RFP for each milestone payment.

Payment shall be made to the Bidder/SELLER on acceptance of receipt after due diligence. The payment will be made on production of the following documents duly certified by the Buyer/Customer/Authority:

i. Commercial Invoices
ii. Inspection Certificate.
iii. Packing list
iv. Store Receipts
v. Insurance documents.

a. **Documents to be submitted:**

The payment of bills will be made on submission of the following documents by the Seller to the Paying Authority along with the bill:

i. Ink-signed copy of Commercial invoice / Seller's bill.
ii. Copy of Supply Order
iii. Inspection note.
iv. Claim for statutory and other levies to be supported with requisite documents / proof of payment.
v. Exemption certificate for Excise duty / Customs duty, if applicable.
vi. Advance Bank Guarantee if advance is claimed.
vii. Guarantee / Warranty certificate.
viii. Performance Bank guarantee / Indemnity bond where applicable.
ix. DP extension letter.
x. Details for electronic payment viz Account holder's name, Bank name, Branch name and address, Account type, Account number, IFSC code, MICR code (if these details are not incorporated in supply order/contract).
xi. Any other document / certificate that may be provided for in the Supply Order / Contract.

xii. User Acceptance/ certification from the end user at the respective sites for all the milestones payments.

(Note – From the above list, the documents that may be required depending upon the peculiarities of the procurement being undertaken, and the milestone reached may be included)

b. **Fall clause.**

The following Fall clause will form part of the contract placed on successful Bidder: -

i. The price charged for the stores supplied under the contract by the Seller shall in no event exceed the lowest prices at which the Seller sells the stores or offers to sell stores of identical description to any persons/Organisation including the purchaser or any department of the Central government or any Department of the State government or any statutory undertaking of the central or state government as the case may be during the period or till the performance of all Supply Orders placed during the currency of the Purchase Order is completed.

ii. If at any time, during the said period the Seller reduces the sale price, sells or offer to sell such stores to any person/organisation including the Buyer or any PU Deptt, of Central Govt. or any Department of the State Government or any Statutory undertaking of the Central or state Government as the case may be at a price lower than the price chargeable under the contract, he shall forthwith notify such reduction or sale or offer of sale to the Purchase / Contracting Authority and to the Director general of Supplies & Disposals and the price payable under the contract for the stores of such reduction of sale or offer of the sale shall stand correspondingly reduced. The above stipulation will, however, not apply to:-

1) Exports by the Seller.
2) Sale of goods as original equipment at price lower than the prices charged for normal replacement.
3) Sale of goods such as drugs which have expiry dates.
4) Sale of goods at lower price on or after the date of completion of sale/placement of the order of goods by the authority concerned under the existing or previous Purchase Orders as also under any previous contracts entered into with the Central or State Govt. Depts, including their undertakings excluding joint sector companies and/or private parties and bodies.

6. Guidelines to the Vendors

1. Vendor shall comply with all specifications of this RFP / supply order. Any deviations compared to this RFP / supply order specifications shall be mentioned clearly in their offer and supported with justification on how these deviations will / will not hamper the overall performance of the system. Any improvement in the offered system compared to RFP specification shall be separately brought out in the offer.
2. The overall configuration and implementation plan should be clearly explained with the help of block schematic of the complete system.
3. The vendor must provide a Statement of Compliance (SoC), covering each point of system and sub-system specifications. In case of any discrepancy between OEM data-sheet and compliance statement, OEM data-sheet will be considered final and binding. This SoC should be well supported by documentation consisting of data sheets, brochure, calculations, literature etc. All relevant details of each subsystem like make & model number, detailed specifications, block schematic, etc. should also be provided. NSIL reserves right to reject any incomplete offer.
4. At the time of installation and commissioning of the system if it is found that some additional hardware or software elements are required to complete the configuration to meet the total system requirement; which were not included in the vendor's original list of deliverables; then vendor is required to supply such items to ensure the completeness of the configuration at no extra cost.
5. After receiving the offers, Vendors will be invited, if required, to make technical presentation on their offer to the technical evaluation committee at NSIL. Vendors will be required to provide clarification, if called for, by the evaluation committee, on any matter related to offer.
6. During implementation and warranty and CAMC support period, if it is observed that any of the supplied components of the system (software and hardware) are not able to handle load or its performance is not able to meet the functional requirements/ technical specifications given in the Tender, the vendor at its own cost shall replace that component (software or hardware) with better specification equipment or provide additional Hardware (along with Operating System)/software components/Licenses for meeting the technical specifications and user requirements within reasonable time period.
7. The vendor shall understand that there is scope of minor changes in configuration / functionalities in upgradation of IT Infrastructure. The vendor shall accommodate such changes during development or acceptance or activities at no extra cost. The vendor is also responsible for resolving any operational issues.
8. No data, during testing and operational phase, shall be disclosed to any outside party without the consent of User/NSIL. The data shall be treated as confidential.
9. Bidder shall be fully responsible for the manufacturer’s warranty in respect of proper design, quality and workmanship of overall hardware, software, accessories, etc., covered by the offer. The bidder must cover warranty for all hardware equipment, software, accessories, etc., against any manufacturing defects/malfunctioning during the Warranty period. During the warranty period and CAMC period, the bidder shall maintain the hardware, software, accessories, and repair / free of cost.

10. If faulty equipment is not repairable, successful bidder shall intimate NSIL/Customer regarding replacement of faulty unit, giving all the details/ specifications of the replacement unit. Consent from NSIL/Customer shall be obtained before replacement.
11. NSIL reserves the right to inspect and monitor/ assess the progress/ performance of the work / services at any time during the course of the Contract / supply order. NSIL / user may demand and upon such demand being made, Vendor shall provide documents, data, material or any other information which NSIL / user may require, to enable it to assess the progress/ performance of the work / service.
12. Vendor's Team shall comply and indemnify NSIL with the provision of all laws including labour laws, rules, regulations and notifications issued there under from time to time. All safety and labour laws enforced by statutory agencies and by competent authority shall be applicable in the performance of this Contract and Vendor's Team shall abide by these laws. The Vendor shall also submit the compliance of the laws along with techno-commercial proposal.
13. Based on the location of the site, access to the Site shall be restricted. No access to any person except the essential and required members of Vendor's Team who are authorized by NSIL / user and are genuinely required for execution of work or for carrying out management/ maintenance shall be allowed entry. Even if allowed, access shall be restricted to the pertaining the specified work under supply order only.
14. In the event of NSIL noticing at any time that any amount has been disbursed wrongly to Vendor or any other amount is due from Vendor to the NSIL, NSIL may without prejudice to its rights recover such amounts by other means after notifying Vendor or deduct such amount from any payment falling due to the Vendor. The details of such recovery, if any, shall be intimated to the Vendor. The Vendor shall receive the payment of undisputed amount under subsequent invoice for any amount that has been omitted in previous invoice by mistake on the part of NSIL or the Vendor.
15. All payments to Vendor shall be subject to the deductions of tax at source under Income Tax Act, and other taxes and deductions as provided for under any law, rule or regulation. All costs, damages or expenses which NSIL may have paid or incurred, for which under the provisions of the Contract / supply order, Vendor is liable, the same shall be deducted by NSIL from any dues to Vendor. All payments to Vendor shall be made after making necessary deductions as per terms of the Contract and recoveries towards facilities, if any, provided by NSIL to Vendor on chargeable basis.
16. Vendor shall fully familiarize themselves about the applicable domestic taxes (such as CGST, SGST, IGST, etc.) on amounts payable by NSIL under this contract / supply order. All such taxes must be included by Vendors in the financial proposal. (Vendor to find out applicable taxes for the components being proposed.)

7. Indemnity

Vendor shall indemnify NSIL or its users from and against any costs, loss, damages, expense, claims including those from third parties or liabilities of any kind howsoever suffered, arising or incurred inter alia during execution of the supply order. Vendor shall indemnify NSIL or its users on account of:

- Any negligence or wrongful act or omission by Vendor or any third party associated with Vendor in connection with or incidental to this supply order; or

- Any breach of any of the terms of Vendor's responsibility as agreed for the RFP and supply order under Framework contract by Vendor.
- Any infringement of patent, trademark/copyright or industrial design rights arising from the use of the supplied goods and related services or any part thereof.
- Vendor shall also indemnify NSIL against any privilege, claim or assertion made by a third party with respect to right or interest in, ownership, mortgage or disposal of any asset, property etc.
- Regardless of anything contained (except for the Vendor's liability for bodily injury and/ or damage to tangible and real property for which it is legally liable and it's liability for patent and copyright infringement in accordance with the terms of this Agreement) the total liability of Vendor, is restricted to the total value of the supply order and Vendor is not responsible for any third party claims.

8. Arbitration:

Differences and disputes, if any arising between NSIL and the bidder at the time of execution of the assignment shall be settled mutually. Unsettled disputes, if any, shall be referred to a single / sole arbitrator to be appointed by Chairman-cum-Managing Director, NSIL, whose decision shall be binding on both the parties. The arbitration proceedings shall be governed by Indian Arbitration & Conciliation Act 1996 and the rules thereunder or any statutory modifications thereof for the time being in force. The venue of the arbitration shall be Bengaluru. The expenses of the arbitration shall be equally shared or shall be as per the decision of the Arbitrator.

9. Force Majeure Clause.

Neither party shall bear responsibility for the complete or partial non-performance of any of its obligations (except for failure to pay any sum which has become due on account of receipt of goods under the provisions of the present contract), if the non-performance results from such Force Majeure circumstances as Flood, Fire, Earth Quake and other acts of God as well as War, Military operation, blockade, Acts or Actions of State Authorities or any other circumstances beyond the parties control that have arisen after the conclusion of the present contract.

Section-3: Annexure's

Annexure-A: Covering Letter

(To be given in the Company Letter Head by the authorized representative of the Bidder)

To

Deputy Manager (Commercial)
NewSpace India Limited (NSIL)
ISRO HQ Campus, New BEL Road
Bengaluru-560 094, Ph: 080-2322 7777
E-mail: purcahse@nsilindia.co.in

Sub: Contract for Supply, Installation, Commissioning, Operation and Maintenance of upgradation of IT infrastructure for NSIL users - Reg.

Dear Sir,

1. Having examined the Tender document and appendix thereto, we would like to clearly state that we qualify for the work envisaged under this Tender and meets all eligibility criteria indicated in the Tender document.
2. I/We are in conformity with the Tender document and offer "Purchase Order for Supply, Installation, Commissioning, Operation and Maintenance of upgradation of IT Hardware for NSIL users" as per the Tender document and the terms and condition. If selected, we offer to Supply, Install, Commission, Operate and Maintain the work allotted to us as per the scope of the RFP within the time frame specified for the work. We would NOT outsource the work to any other associate / franchisee/ third party under any circumstances without prior approval of NSIL.
3. I/We agree to execute an agreement, in the form to be communicated by NSIL, incorporating all agreements with such alterations or additions thereto as may be necessary to adapt such agreement to the circumstances of the standard and notice of the award within time prescribed after notification of your intention to accept this Proposal.
4. I/We understand that if the details given in support of claims made above are found to be untenable or unverifiable or both, our Proposal may be rejected without any reference to us. We further clearly understand that NSIL is not obliged to inform us of the reasons of rejection of our Proposal.
5. It is certified that the information furnished in this Proposal is true and correct to the best of our knowledge and nothing has been concealed or tampered with.
6. I am duly authorized to sign the documents/ Proposal for and on behalf of our Company/ Firm. Checklist, Company details, Undertaking Form and Technical Specifications as per the template are enclosed herewith.

Date:	Signature:
	Name
Place:	Designation
	Official stamp

Annexure-B: Check List

Sub: Purchase Order for Supply, Installation, Commissioning, Operation and Maintenance of upgradation of IT infrastructure for NSIL users

Check List for Relevant Documents to be submitted

S. No.	Document	Attached (Yes/No)
01	Bid document cost (Demand Draft)	
02	Enclose copy of Bidder registration details with date of incorporation.	
03	Copy of Memorandum and Articles of Association / Partnership Deeds	
04	Documents requested in Section-1 clause 2.5 and Section-2 clause 1.	
05	Address of registered Site Works/ Workshop etc.,	
07	Copy of Latest filed tax returns	
08	All Annexure's (A, B, C, D, E, F, G, H)	
09	ISO 9001:2015 Certification and other certifications, if any. Copy to be enclosed.	
10	Signed and scanned copy of complete Tender document	
11	Integrity Pact	
12	All other applicable documents as per RFP Document A and Document B	

Signature of authorized representative
With Office Seal

Date: ----------

Annexure-C: Undertaking Form

(To be given in the Company Letter Head
by the authorized representative of the Bidder)

To

Deputy Manager (Commercial)
NewSpace India Limited (NSIL)
ISRO HQ Campus, New BEL Road
Bengaluru-560 094
Ph: 080-2322 7777
E-mail: purcahse@nsilindia.co.in

Dear Sir,

Sub: Purchase Order for Supply, Installation, Commissioning, Operation and Maintenance of upgradation of IT Infrastructure for NSIL users

I / We hereby declare that our Firm/ Company, at the time of bidding:

a) possess the necessary professional, technical, financial, and managerial resources and competence as required in this Tender
b) is having unblemished record and is not declared ineligible for corrupt & fraudulent practices either indefinitely or for a particular period of time by any State/ Central government/ PSU/ UT.
c) is not insolvent in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and is not the subject of legal proceedings for any of the foregoing reasons.
d) Has read and understood the Tender document and comply with the terms & conditions of the Tender.
e) Information provided in the Proposal submitted to NSIL is correct and true to best of my/ our knowledge.

Signature:

Date:

Name

Place:

Designation

Official stamp

Annexure-D: Bank Guarantee Format

WHEREAS M/s._____(Name & Address of the Firm) having their registered office at _____ (Address of the firms Registered office) (Hereinafter called the 'bidder') wish to participate in the tender No. _____
for _NewSpace India Limited (NSIL) and WHEREAS a Bank Guarantee for (Hereinafter called the "Beneficiary") Rs. _____ (Amount of BG) valid till_____ (Mention here date of validity of this Guarantee which from the date of the submission of Tender's offer) which is required to be submitted by the bidder along with the tender.

We, _____ (Name of the Bank and address of the Branch giving the Bank Guarantee) having our registered office at _____ (address of Bank's Registered office) hereby give this Bank Guarantee No. _____ dated _____ and hereby agree unequivocally and unconditionally to pay immediately on demand in writing from the NewSpace India Limited or any officer authorized by it in this behalf any amount not exceeding Rs. (Amount for specific supply order), (Rupees _____ (In words) to the said NewSpace India Limited on behalf of the bidder.

We _____ (Name of the Bank) also agree that withdrawal of the tender or specific supply order by the bidder within its validity or Non submission of Security Deposit by the bidder within one month from the date supply order has been accepted by the NewSpace India Limited would constitute a default on the part of the bidder and that this Bank Guarantee is liable to be invoked and encashed within its validity by the Beneficiary in case of any occurrence of a default on the part of the bidder and that the encashed amount is liable to be forfeited by the Beneficiary.

This agreement shall be valid and binding on this Bank up-to and inclusive of _____ (mention here the date of validity of Guarantee) and shall not be terminable by notice or by Guarantor change in the constitution of the Bank or the firm of bidder or by any reason whatsoever and our liability hereunder shall not be impaired or discharged by any extension of time or variations or alternations made, given, conceded with or without our knowledge or consent by or between the bidder and the NSIL.

"Notwithstanding anything contrary contained in any law for the time being in force or banking practice, this Guarantee shall not be assignable, transferable by the beneficiary (i.e. NSIL). Notice or invocation by any person such as assignee, transferee or agent of beneficiary shall not be entertained by the Bank. Any invocation of the Guarantee can be made only by the beneficiary directly.

NOT WITHSTANDING anything contained hereinbefore, our liability under this guarantee is restricted to Rs. _____ (Amt. of supply order) (Rupees_____) (in words). Our Guarantee shall remain in force till _____ (Date of validity of the Guarantee). Unless demands or claims under this Bank Guarantee are made to us in writing on or before _____(Date of validity of the Guarantee), all rights of Beneficiary under this Bank Guarantee shall be forfeited and we shall be released and discharged from all liabilities there under:

Place:

Date:

-Please mention here Complete Postal Address of the Bank with Branch Code, Telephone and Fax Nos.

SIGNATURE OF THE BANK'S
AUTHORISED SIGNATORY WITH
OFFICIAL ROUND SEAL

NAME OF DESIGNATED BANKS:

Note1: The Bank Guarantee (B.G) Shall be from the Nationalize Banks or any other Banks, as Notified by the Finance Department, from time to time.

Note2: The B.G shall be signed by two bank officers Jointly if the amount of B.G is more than Rs 50,000/- and B.G must have proper B.G number as per R.B.I guidelines.

Note 3: Similar format to be used for ABG.

Annexure-E: Declaration of Local Content

(To be given in the Company Letter Head
by the authorized representative of the Bidder)

Dated …….

I/We,M/s……,
address……, hereby undertakes and declare that the proportion of imported content to Domestic content in terms of percentage (%) of the total value of quoted item/s are as follows –

Domestic Content (%) –
Imported Content (%) –

It is also declared that the value addition for the material supplied/ to be supplied is made at following locations:
a) ……
b) …….
c)……
d)…….

We also understand that the false declarations will be in breach of the code of Integrity under rule 175(1)(i)(h) of the General financial rules for which a bidder or its successors can be debarred for up to two years as per Rule 151(iii) of the General Financial Rules along with such other actions as may be permissible under law.

Signature:

Date:

Name

Place:

Designation

Official stamp

Annexure-F: Integrity Pact

Pre-Contract Integrity Pact

This Pact made this ..... day of ..... between NewSpace India Limited, a body corporate constituted by the Central Government and having its Corporate Office at ----------, hereinafter called the Authority (which term shall unless excluded by or is repugnant to the context, be deemed to include its Chairman cum Managing Director, or Executive Director, Directors, officers, or any of them specified by the Chairman cum Managing Director in this behalf, and shall also include its successors and assigns) of the one part

AND

Represented by of the other part, hereinafter called the "Bidder/Contractor" (which term shall unless excluded by or is repugnant to the context be deemed to include its heirs, representatives, successors and assigns of the Bidder/ Contractor)

WHEREAS the Authority intends to award, under laid down organizational procedures, tender/ contract for The Authority, while discharging its functions on business principles, values proper compliance with all relevant laws and regulations, and the principles of natural justice, ethics, equity, fairness and transparency in its relations with the Bidders/ Contractors.
WHEREAS the Authority is desirous to make its business mechanism more transparent, thus to ensure strict adherence of the aforesaid objectives/goals, the Authority hereby adopts the instrument developed by the renowned international non-governmental organization "Transparency International" (TI) headquartered in Berlin (Germany). The Authority will appoint an Independent External Monitor (IEM) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.
AND WHEREAS the Bidder is submitting a tender to the Authority for …… In response to the NIT (Notice Inviting Tender) dated ..... Contractor is signing the contract for execution of .....

NOW, therefore,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to enabling the Authority to obtain the desired said stores/equipment/execution of works at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling Authority to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the Authority will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:

Commitments of the Authority;

The Authority undertakes that no official of the Authority, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favor or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

All the officials of the Authority will report to the appropriate authority office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the Authority with full and verifiable facts and the same is prima facie found to be correct by the Authority, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the Authority and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the Authority the proceedings under the contract would not be stalled.
Commitments of Bidders/Contractor.

The Bidder/ Contractor commits itself to take all measures necessary to prevent corrupt practice, unfair means and illegal activities during any stage of its bid or during any pre-contract or post- contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following: -

The Bidder/Contractor will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Authority, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

(i) The Bidder/Contactor further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Authority or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Authority for showing or forbearing to show favor or disfavor to any person in relation to the contract or any other contract with the Authority.

(ii) The Bidder / Contactor has not entered and will not enter with other bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specification, certifications, subsidiary contracts, submission or non-submission of bids or any actions to restrict competitiveness or to introduce cartelization in the bidding process.
The Bidder/Contractor shall, when presenting his bid, disclose the name and address of agents and representatives and Indian BIDDERS shall disclose their foreign principals or associates.
The Bidder/ Contactor shall when presenting his bid disclose any and all the payments he has made or, is committed to or intends to make to agents/brokers or any other intermediary, in connection with this bid/contract.

The Bidder/Contractor, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the Authority or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

The Bidder/Contractor will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

The Bidder/ Contractor will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

The Bidder / Contactor shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the Authority as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The Bidder / Contractor also undertakes to exercise due and adequate care lest any such information is divulged.

The Bidder/ Contractor will inform to the Independent External Monitor.
If he receives demand for an illegal/ undue payment/benefit.
If he comes to know of any unethical or illegal payment/ benefit.
If he makes any payment to any Authority's associate(s)
The Bidder/ Contactor commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
The Bidder/ Contactor shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

If the Bidder/ Contractor or any employee of the Bidder/ Contractor or any person acting on behalf of the Bidder/ Contractor, either directly or indirectly, is a relative of any of the officers of the Authority, or alternatively, if any relative of an officer of the Authority has financial interest/ stake in the Bidder's/ Contractor's firm, the same shall be disclosed by the Bidder/ Contractor at the time filing of tender. The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1956.

The Bidder/ Contractor shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the Authority.

That if the Bidder/ Contractor, during tender process or before the award of the contract or during execution of the contract/ work has committed a transgression in violation of section 2 or in any other form such as to put his reliability or credibility as Bidder/ Contractor into question, the Authority is entitled to disqualify him from the tender process or to terminate the contract for such reason and to debar the BIDDER from participating in future bidding processes.

The Bidder/Contractor agrees that if it makes incorrect statement on this subject, he can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason and he may be considered for debarment for future tender/contract processes.

That sub-contractor(s)/ associate(s) engaged by the Contractor, with the approval of the Authority after signing of the contract, and whose value of the work contribution exceeds Rs 2 Crores. (Rupees Two Crores) will be required to sign this Pact by the Contractor, and the same will be submitted to the Authority before doing/ performing any act/ function by such sub-contractor(s)/ associate(s) in relation to the contract/ work.

That the Authority will disqualify from the tender process all Bidder(s) who do not sign this Pact or violate its provisions or fails to get this Pact signed as per the RFP terms and conditions.
That if the Contractor(s) does/ do not sign this Pact or violate its provisions or fails to get this Pact signed as per the RFP terms and conditions. Authority will terminate the contract and initiate appropriate action against such Contractor(s).

Sanctions for Violations/ Disqualification from tender process and exclusion from future Contracts.
Any breach of the aforesaid provisions by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the Authority to take all or any one of the following actions, wherever required:

To immediately call off the pre-contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.

To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.

If the Authority has disqualified/ debarred the Bidder from the tender process prior to the award under section 2 or 3 or 4, the Authority is entitled to forfeit the Earnest Money Deposited.

To recover all sums already paid by the Authority, with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India. If any outstanding payment is due to the BIDDER from the Authority in connection with any other contract or any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.

To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the Authority resulting from such cancellation/rescission and the Authority shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.

To debar the BIDDER from participating in future bidding processes for a minimum period of three years, which may be further extended at the discretion of the Authority.

To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

In case where irrevocable Letters of Credit have been received in respect of any contact signed by the Authority with the BIDDER, the same shall not be opened.

Forfeiture of Performance Bank Guarantee in case of a decision by the Authority to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

That the Bidder / Contractor agrees and undertakes to pay the said amount without protest or demur subject only to condition that if the Bidder/ Contractor can prove and establish to the satisfaction of the Authority that the disqualification / debarment of the bidder from the tender process or the termination of the contract after award of the contract has caused no damage to the Authority.

The Authority will be entitled to take all or any of the actions mentioned above of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

That if the Bidder/ Contractor applies to the Authority for premature revocation of the debarment and proves to the satisfaction of the Authority that he has installed a suitable and

effective corruption prevention system and also restored/ recouped the damage, if any, caused by him, the Authority may, if thinks lit, revoke the debarment prematurely considering the facts and circumstances of the case, and the documents/ evidence adduced by the Bidder/ Contractor for first time default.

That a transgression is considered to have occurred if the Authority is fully satisfied with the available documents and evidence submitted along with Independent External Monitor's recommendations/ suggestions that no reasonable doubt is possible in the matter.

The decision of the Authority to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent External Monitor(s) appointed for the purpose of this Pact.

Allegations against Bidders/ Contractors/ Sub-Contractors/ Associates:

That if the Authority receives any information of conduct of a Bidder/ Contractor or Sub-Contractor or of an employee or a representative or an Associates of a Bidder, Contractor or Sub-Contractor which constitute corruption, or if the Authority has substantive suspicion in this regard, the Authority will inform the Vigilance Department for appropriate action.

Facilitation of Investigation.

In case of any allegation of violation of any provisions of this Pact or payment of commission, the Authority or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such Examination.

Law and Place of Jurisdiction.

That this Pact is subject to Indian Law. The place of performance jurisdiction is the Corporate Headquarter of the Authority, as applicable. The courts at Bengaluru shall have exclusive jurisdiction to adjudicate any dispute which may arise in relation to this tender or any way connected or incidental to this tender/Pact.

Other Legal Actions

That the changes and supplements as well as termination notices need to be made in writing.
Pact duration (Validity)

13.1 That this Pact comes into force when both the parties have signed it. It expires for the Contractor 12 months after the final payment under the respective contract, and for all other Bidders 3 months after the contract is awarded.

13.2 That if any claim is made/ lodged during this period, the same shall be binding and continue to be valid despite the lapse of this Pact as specified herein before, unless it is discharged/ determined by Chairman cum Managing Director of the Authority.

13.3 That should one or several provisions of this Pact turn out to be invalid; the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

Company Code of Conduct

Bidders are also advised to have a company code of conduct (clearly rejecting the use of bribe and other unethical behavior) and a compliance program for the implementation of the code of conduct throughout the company.

The parties hereby sign this Integrity Pact at on

AUTHORITY:	BIDDER:
Name of the Officer: Designation Witness	Name (Authorized Signatory): Designation: Witness:

Annexure-G: Non-Disclosure Agreement (NDA)

(To be made on Stamp Paper of value INR 100)

THIS NON-DISCLOSURE Agreement made at Bengaluru, India on this 2nd day of May 2025 between NewSpace India Limited a company registered under the Companies Act, 2013 and having its registered office at ISRO HQ Campus, Bengaluru – 560 094 (hereinafter referred to as "NSIL") and _____a company registered under the Companies Act, 2013 and having its registered office_____, India (hereinafter referred to as "_____").
NSIL and shall hereinafter be collectively referred to as "the Parties" and individually as "a Party".

WHEREAS

A. NSIL has floated a tender and is required to provide certain information to **"Bidder** Name" execute the contract

B. The Parties intend that the aforesaid information be kept confidential as between the Parties. The Parties undertake and declare that they shall not divulge, publish or reproduce the same before any party or person except in accordance with the terms of this Agreement.

NOW THEREFORE the parties agree as follows

1. As used in this Agreement (hereinafter referred to as the "Agreement") the term "Confidential Information" shall mean any technical, confidential, proprietary or trade secret information or data disclosed by the Disclosing Party in connection with the Project to the Receiving Party including without limitation any written or printed documents, specifications, designs, technical details, facility layouts, general arrangement plans, production schedules, drawings, samples, models, information regarding operations, financial information, strategies, either in writing or orally or any means of disclosing such Confidential Information that the Disclosing Party may elect to use prior to the execution or during the validity of this Agreement. The Receiving Party agrees that all Confidential Information shall be treated as absolute confidential and the Receiving Party shall not disclose to any person such information otherwise than in terms of this agreement. The receiving Party will impose a similar duty of confidentiality on any employee to whom the Receiving Party is permitted to transfer such information in accordance with the terms hereof.
   For the purposes of this Agreement, the term "Receiving Party" shall mean and include its officers, employees, directors, agents, contractors, representatives, affiliated companies, successors and assigns provided any claim in connection with the Agreement shall only be made against _____(the receiving party).

2. Nothing in this Agreement may be construed as compelling the Disclosing Party to disclose any Confidential Information to the Receiving Party or to enter into any contractual relationships with the Receiving Party.

3. Any information or data in whatever form disclosed by the Disclosing Party to the Receiving Party and which (i) is clearly identified as Confidential Information by an appropriate and conspicuous marking or (ii) has been identified as Confidential Information at the time of disclosure shall be subject to the relevant terms and conditions of this Agreement. The Disclosing Party's decision whether any information disclosed by it under this Agreement is confidential or not shall be final and binding on the Receiving Party.

4. The Receiving Party hereby covenants that the Confidential Information received from the Disclosing Party shall:
   (a) Be safely kept by the Receiving Party; the Receiving Party shall protect the Confidential Information with the same degree of care as the Receiving Party uses with its own

confidential information in order to prevent its disclosure, copy and / or its use (but in no event less than reasonable care) for purposes other than the Proposal.

(b) Be only disclosed to, and used by, those employees or directors who have a need to know.

(c) Not be disclosed to a third party except those with a need to know provided they receive such information subject to the same restrictions as are contained in this Agreement.

(d) Be used by the Receiving Party directly or indirectly, solely for the purpose of execution of the project

5. The Receiving Party shall promptly upon requests by the Disclosing Party at any time return all copies of the Confidential Information communicated to it hereunder together with all copies and extracts made thereof and shall not retain any copies of the same, in any form whatsoever except for one copy for its professional records purposes subject to confidentiality obligations herein.

6. The Receiving Party shall have no obligations or restrictions with respect to:

(a) Information publicly known through no wrongful act of the Receiving Party.

(b) Information rightfully disclosed by a third party without breach of this Agreement by the Receiving Party and which can be communicated without restriction.

(c) Information which was already known, or which was independently developed by the Receiving Party (provided that the Receiving Party can demonstrate the same).

(d) Information, the disclosure of which the Disclosing Party authorizes in writing.

7. Nothing in this Agreement shall be construed as granting to the Receiving Party any patent, copyright or design license, or rights of use under similar intellectual property rights in respect of the Confidential Information.

8. The Receiving Party shall not without prior written consent of the Disclosing Party:

(a) Disclose to any person, directly or indirectly:

(b) The fact that the Confidential Information has been made available to the Receiving Party by the Disclosing Party or that the Receiving Party has inspected any portion of the Confidential Information; or

(c) The fact that any discussion or negotiation is taking place concerning the Project; or

(d) Any of the terms, conditions or other facts with respect to the Project, including the status thereof; or

(e) Make any private or public announcement or statement concerning or relating to the Project.

9. The Disclosing Party represents and warrants that save as otherwise notified in writing to the Receiving Party:

(a) Disclosure of information by it to the Receiving Party does not infringe the rights of any third party nor is it under any restriction with regard to the disclosure of any information, and that where applicable, it has obtained all licenses and consents necessary to enable the lawful disclosure of information by it to the Recipient; and.

(b) It is not aware of any restriction on the use of such information by the Receiving Party, save as provided in this Agreement.

(c) To the effect that the foregoing representations and warranties shall be deemed to be given at the date of this Agreement and after that date upon and in respect of each disclosure. The Disclosing Party makes no warranty or representation whatsoever as to the accuracy, completeness, suitability or adequacy of any information or as to the results obtained from it and assumes no responsibility in respect of the use of the information by the Receiving Party.

10. The Receiving Party shall be liable to the Disclosing Party for such loss, damage, costs, expenses or liabilities arising out of any such action, claim or proceeding, brought by any third party pursuant to any unauthorized disclosure or use of any information by the Receiving Party, or by any person for whom the Receiving Party is responsible under this Agreement, or pursuant to

any breach of any undertaking, warranty or representation contained in this Agreement as awarded by a court of competent jurisdiction. The Disclosing party will revoke the bank guarantee in case of any breach.

11. For the purposes of this Agreement 'Classified Information' shall mean information, documents and material of any kind which the respective Government i.e. Indian Government has given or caused to be given a security classification irrespective of whether the same is transmitted orally, electronically, in writing or by hand. Notwithstanding any other provision of this Agreement:
    (a) Each Party hereto undertakes to follow security procedures prescribed for military purposes with respect to disclosure, receipt, production, use and handling of Classified Information as notified by Disclosing Party.
    (b) Any Classified Information, disclosed by one Party hereto shall be, whatever the method of disclosure be, identified by the Disclosing Party as Classified Information at the time of disclosure.
    (c) The provisions of this Clause are to remain in full force and effect notwithstanding any termination by expiration or otherwise of this Agreement.

12. In the event the Receiving Party is required to disclose Confidential Information under any provision of law or upon an action, subpoena or order of a court of competent jurisdiction or of any requirement of legal process regulation or governmental order, decree, regulation or rule, the Receiving Party will immediately notify the Disclosing Party of its having received a request to so disclose (along with the terms and circumstances thereof), unless otherwise prohibited by law and consult with the Disclosing Party on action or steps to be taken in response to such request.

13. This Agreement shall be valid for a period of three years from the date of its execution between the parties. Notwithstanding the aforesaid, the obligations of Parties in connection with confidentiality under this Agreement shall survive in perpetuity.

14. The foregoing constitutes the entire Agreement between the Parties with respect to the subject matter hereof and supersedes and cancels any prior representation, understanding and commitment (whether oral and written) made between the Parties with respect to or in connection with any of the matter of things to which this Agreement applies.

15. This Agreement shall be governed by and shall be interpreted in accordance with the laws of India.

16. Any dispute arising in connection with or out of the validity, performance or the interpretation of this Agreement shall be finally settled by the competent jurisdiction in Bengaluru.

17. The Receiving Party acknowledges that any breach of the terms and conditions of this Agreement may cause the Disclosing Party irreparable damage for which recovery of money damages would be inadequate. Therefore, the Receiving Party agrees that the Disclosing Party shall be entitled, in addition to any other remedies available to it, to seek injunctive relief and/or other equitable relief to prevent or restrain any breach by the Receiving Party or its employees/officials, or otherwise to protect its rights, under this Agreement.

18. Unless otherwise provided herein, all notices or other communications under or in connection with this Agreement shall be given in writing and may be sent by personal delivery or post or courier or facsimile at the address as specified herein below:

To NSIL			To M/s	
Address			Address	
Phone No			Phone No	
E-mail			E-mail	

Any such notice or other communication will be deemed to be effective if sent by personal delivery, when delivered, if sent by post, 4 (four) days after being deposited in the post and if sent by courier, one day after being deposited with the courier, and if sent by facsimile, when sent (on receipt of a confirmation to the correct facsimile number).

IN WITNESS WHEREOF, this Agreement is executed by authorized representatives of both the Parties in two (2) originals.

Signed by the within M/s_____

In the presence of

Signed by the within M/s NSIL

In the presence of

Annexure - H: Land Border Sharing Declaration

(To be submitted in the bidder's letter head)

In-line with Department of Expenditure's (DoE) Public Procurement Division Order vide ref. F.No.6/18/2019-PPD dated 23.07.2020 & 24.7.2020 regarding restrictions under Rule 144 (XI) of the General Financial Rules (GFRs), 2017

Tender no . ……..

Job: ……..

"I/ we have read the clauses pertaining to Department of Expenditure's (DoE) Public Procurement Division Order (Public procurement no 1, 2 & 3 vide ref. F.No.6/18/2019-PPD dated 23.07.2020 & 24.7.2020) regarding restrictions on procurement from a bidder of a country which shares a land border with India.

I/We hereby certify that I/ we the bidder < name of the bidder……> is / are

a) Not from such a country and eligible to be considered for this tender.

OR

b) From such country, has been registered with the competent authority and eligible to be considered for this tender. (Evidence of valid registration by the competent authority shall be attached)

For and behalf of _____ (Name of the bidder)

(Signature, date & seal of authorized representative of the bidder)"

REQUEST FOR PROPOSAL

RFP No NSIL/RFP/IT/UPG/ 2025/01

DOCUMENT B

(Technical Document)

Supply, Installation, Commissioning, Operation and Maintenance of

Upgradation of IT Infrastructure

NewSpace India Limited (NSIL)
A Govt. of India company under Department of Space, Govt. of India
Brigade Rubix, Watch Factory Road, Yeshwanthpur
Bangalore – 560013, INDIA

Table of Contents

Chapter 1:

1.1 Introduction:

This RFP seeks Technical and Commercial proposal from qualified vendors for the Supply, Installation, Integration, Testing, Commissioning and Post Warranty Comprehensive Annual Maintenance Services (CAMS) for the entire IT infrastructure as per the scope of this RFP.

1.2 List of Deliverables

List of deliverables/ items / service required along with technical specification for hardware and services, which is required to be delivered as part of the scope is as follows:-

Ser	Description	Qty	Technical Spec / Requirement*
1	Workstation	54	Appendix 'A'
2	Monitor	74	Appendix 'B'
3	NAS Storage (250 TB)	1	Appendix 'C'
4	Tape Backup	1	
5	Server (Rack) - Config-1	24	Appendix 'D'
6	Edge Switch	32	Appendix 'E'
7	Core Switch	2	Appendix 'F'
8	UTM/NGFW-Config-1	2	Appendix 'G'
	UTM/ NGFW - Config-2	6	
	UTM Hardware Authentication Token	20	
9	NGFW Logger & Traffic Analyser	1	
10	NGFW Manager	1	
11	End Point Protection & Management Tool	150	
12	Interconnect Router - Config-1	2	Appendix 'H'
13	Interconnect Router - Config-2	4	
14	Server Room Structured	1	Appendix 'I'

	Cabling and Accessories		
15	All-in-one PC	6	Appendix ‘J’
16	NMS Laptop	2	Appendix ‘K’
17	ATS Device	8	Appendix ‘L’
18	STC Server Node	8	Appendix ‘M’
19	MCP Server	6	Appendix ‘N’
20	Thin Client AIO	14	Appendix ‘M’ & ‘N’
21	LCD Display with Trolley / Wall mount (75 inch)	3	Appendix ‘O’
22	Syslog Servers - Config-2	5	Appendix ‘P’
23	SIEM Server/ Security Analytics Server - Config-3	3	Appendix ‘Q’
24	Printer - Color	2	Appendix ‘R’
25	Printer - BW	8	Appendix ‘S’
26	NMS Software with Lics	1	Appendix ‘T’
27	RKM	8	Appendix ‘U’
28	KVM (40 Port) - Config-1	1	
	KVM (8 Port) - Config-2	2	
29	SIEM Software with 3500 EPS	1	Appendix ‘V’
30	Network Behavior Analytics (NBA/NBAD)		Appendix ‘W’
31	One Time Implementation + Documentation	1	Appendix ‘X’
32	UT Display	24	Appendix ‘Y’
33	Onsite Support - 2 Skills	For warranty and CAMC period	Appendix ‘Z’
34	Onsite Support - Security Service - 1 Skill	For warranty and CAMC period	

35	Windows Server OS 2022	6	
36	Other Technical Terms and Conditions		Appendix ‘AA’

The table above “List of Deliverables” (not exhaustive), list “include major deliverables for Upgradation of IT Infrastructure system, but are not limited to,”. Bidder to note that the offer needs to include all the items required to realize the IT Infrastructure as per the required configuration and specification.

*The detailed Appendices are in the following section.

Chapter 2: Detailed Specifications of Deliverables

This chapter contains detailed technical specification of all the deliverables.

Appendix 'A' - Workstations

Workstation shall be as per the specifications below:

a. Tower model, RHEL & Windows certified hardware. All the required device drivers for RHEL shall be included in the offer. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

b. **Physical dimension –** The dimension of the workstation (without monitor) shall be strictly within 210 mm x 485 mm x 520mm (W X D X H).

c. **Processor –** One CPU equivalent or better - Intel® Xeon® W5-2465X (16C 3.1 GHz, HT 33.75 MB 200W) or AMD on X86_64 architecture with equivalent or better specification.

d. **Memory -** 128 GB DDR4-2133 ECC Registered memory spread across all memory channels or better configuration

e. **Graphics -** NVIDIA T400 2GB GDDR6 or better. Drivers shall be delivered for RHEL.

f. **Drive Controller –** SAS/SATA controller with Raid 1

g. **Internal Storage –** 2 x 1TB Enterprise SATA HDD in RAID 1 configuration or better shall be offered. HDD shall not be returned back during warranty replacement. DMR to be provided.

h. **Network Controller –** Two independent PCIe network adaptor cards each with dual gigabit Ethernet shall be offered (total 2x2 = 4 nos ports) in addition to the integrated network adaptor port on the motherboard

i. USB keyboard and USB optical mouse to be offered.

j. **Optical Drive –** Internal DVD RW drive

k. Offered workstation shall support dual monitor configuration. Required video cables and / convertors to be offered along with the monitor. All the cables and converters shall be OEM certified component.

l. **Ports –** Front :2 USB, Rear: 4 USB, Audio in, out and Microphone

m. The system shall have integrated sound card and shall have internal Speaker. Should have required multimedia drivers pre-installed.

n. Tool less access to access panel, optical drive, hard drives, expansion cards, processor sockets, memory and internal cables and connectors.

o. **Cooling –** Shall be configured with cooling fans for Power supply, CPU heat sink, and chassis rear or chassis front.

p. **Power–** Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

q. **Certifications –** Following or equivalent international certification are to be provided along with the hardware:

    i. RoHS India [E-Waste (Management) Rules, 2016] certification

    ii. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

    iii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

    iv. Security Compliance – TPM 2.0, UEFI Secure boot

r. **Operating System –** Redhat Enterprise Linux (OEM package of RHEL latest version) Workstation edition to be provided pre-installed in all workstations with three years.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

Appendix ‘B’ - Monitor Specifications

Monitor shall be from same OEM make as of the workstations, the minimum hardware specifications for the monitor is as mentioned below:-

a. 27 Inches (27 inch or 68.5 cm diagonal viewable image size) Monitor

b. Panel Type/ Surface: IPS, LED backlight, antiglare display

c. **Aspect Ratio:** 16:9

d. **Viewing angle:** Upto 178/ 178

e. **Brightness:** upto 350 cd/m2

f. **Contrast Ratio:** Static – 1000:1 static; 2000000:1 dynamic

g. Response Time: 8ms

h. **Pixel Pitch:** 0.233 mm

i. **Color Depth:** 16.7 Million

j. **Native Resolution:** 2560 x 1440

k. **Interface:** Compatible with the offered workstation model suitable to drive dual display configuration.

l. Support for Tilt, Swivel and Pivot rotation

m. Support for VESA mount

n. Each monitor shall be offered with USB powered integrated speaker bar which shall be seamlessly attaches to the monitor’s bezel.

o. Power Supply rating: AC 120/230 V (50/60 Hz)

p. Required video cables / convertors along with the monitor. All cables and convertors shall be OEM certified hardware

s. Monitor to be certified with following or equivalent international certification

    i. RoHS India [E-Waste (Management) Rules, 2016] certification

    ii. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

    iii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'C' - NAS Storage and Backup Infrastructure

Storage shall consist of the following items and as per the specifications detailed below for each item:

No.	Item	Quantity
a.	High Available NAS 250 TB	1 nos
b.	Backup Software (host-based license)	1 nos
c.	Tape Library with Media	1 nos
d.	Backup Server	1 nos
e.	SAN Switch	1 nos

a. High Available NAS

The NAS should offer Unified Storage which supports out of the box capability for different storage protocol under a single management console. The NAS solution offered should be the same product family of a single manufacturer. The storage controller shall be licensed for partitioning / virtual controller / feature for multitenant environment. The Unified Storage Operating System should be owned by the Storage Hardware Manufacturer. The NAS should have High Availability features as mentioned below:

i. The offered solution should be configured with no single point of failure (NSPoF).

ii. The offered solution should be configured with dual controllers which supports Active-Active mode.

iii. The offered solution should provide session/cache information replication across the controllers to support faster failover across the controllers.

iv. It should retain the state information of the active transactions during a controller failover event.

v. Any maintenance activity on the storage, controller OS upgradation, and file system expansion should be performed online without downtime.

vi. Any maintenance activity should be non-destructive for the stored data.

vii. During controller failover shall complete well with in before the client nodes detect file system or storage block is unavailable. Storage which requires remounting of file system or block storage during controller failover event should not be offered.

viii. The NAS configuration should not result in single point of failure at any stage / part failure. Adequate redundancy to be incorporated in the hardware to cater for sustained operations in case of any part failure.

ix. **Physical.** 19 inch Rack mountable Storage hardware along with rack mount kit shall be provided. Such enclosure should permit maintenance access to the subsystems / cards inside without requiring dismounting from the rack.

x. **Protocol Support.** The storage controller should be offered with NFS (v3, v4, v4.1 support), FC, CIFS & iSCSI protocol support. If any additional hardware software is required to support all the required protocol then should be offered in redundancy to ensure NSPoF.

xi. **Disk Enclosure.** The Disk enclosures shall be offered with sufficient capacity to house required number of disks. Specification of the disk enclosure is as mentioned below:

1) The disks offered should be 12Gbps dual ported drives
2) The disk enclosure shall be configured with required interconnection cables to have connectivity with both the controller to avoid single point of failure.
3) The disk enclosure shall be configured with hot swappable redundant power supply and fan tray
4) The usable storage capacity of 250 TB at the file system level should be offered. The offered capacity shall have 230 TB NL-SAS and 20 TB on SSD.
5) Vendor should note that the capacity mentioned above is the usable/workable capacity at the file system level. Vendor should quote for appropriate configuration considering the spares and RAID configuration. For NL-SAS Drive, vendor should consider maximum 12 drives in a RAID group offering 3 disk protection per RAID group. If the solution does not offer 3 Disk protection capability, the solution should be designed with equivalent numbers of disks in global hot spare. The detailed breakup on the disk count to be provided along with the proposal. For NL-SAS drive two global hot spare drive to be offered.
6) The SSD pool can be offered on RAID 6 or on RAID 1 with two global hot spare.
7) Vendor should demonstrate the usable capacity on a Linux NFS client using standard Linux commands like "du -sh".
8) A detailed calculation in arriving at the number of disks to meet the usable storage requirement of 250 TB should be provided along with the offer considering all the penalty in disk group, volume and RAID configuration.
9) Vendor shall include 20% of disk space as file system snapshot reserve area in the file system calculation. The usable capacity shall be derived excluding snapshot reserve area in the file system. Hence 250 TB usable

file system shall have additional 20% disk space reserved/dedicated for snapshot.

10) The storage enclosure shall be populated with **maximum 16 TB Enterprise NL-SAS** and **maximum 4 TB SSD** as performance drive. The vendor can offer lower capacity disk.

11) If vendor is offering higher capacity disk than specified above the total number of disk count shall be as per **16 TB NL SAS and 4TB SSD disk**. Vendor has to offer disks counts accordingly and licenses shall be extended for full capacity.

xii. **Scalability.**

1) The offered storage controller shall be scalable up to 400 drives in a single pair of controllers.

2) The unified proposed system should be field upgradeable to a higher model through data-in-place upgrades

xiii. **Defense against Malware / Ransomware attack.**

1) Product shall offer WORM feature which can be configured on specific volume based on requirement

2) The product shall have capability to block writing malicious files on the disk. Suitable license and configuration to be offered.

3) The product shall have capability to monitor infrastructure for ransom ware attack.

4) The product shall have capability to generate alert for suspicious activity

xiv. **Storage Solution Features and Architecture**

1) The unified storage architecture should be based upon dedicated appliance, running specialized operating system optimized for storage operations.

2) The host operating system in the controller should be strictly based on Unix/Linux based kernel with a specialized environment built to support high performance file service. The storage operating system should not be based on general purpose OS.

3) The proposed Unified storage architecture should not be based upon file services running on general purpose OS and conventional server hardware.

4) The storage should be able to provide single name space/file system for configured capacity and should be scalable upto 256 TB

5) The controller unified storage operating system should be protected by RAID.

6) The controller should support creating disk groups in different RAID levels viz., mirroring, single parity and dual parity or equivalent data protection technologies

7) Each controller should be configured with at least 32 GB of memory.

8) The system should be configured with minimum 4 TB of SSD/Flash/NVMe based cache for accelerating the performance. This SSD or NVMe based pool will not be part of file system.

9) Storage Controller should be capable of supporting a single LUN of size of at least 16 TB.

10) Controllers should support different disk drives viz., SSD, SAS, NL-SAS.

11) It should be possible to grow the file system online.

12) It should be possible to grow the disk pool online to grow the file system.

13) The storage should support data tiering with movement of hot data to high performing drives. It should offer the capability to move data between one tier of drives to another tier of drives.

14) The controller cache should support battery backup option or equivalent technology to protect uncommitted data against power failure.

15) The controller should be configured for point in time images or snapshots and applicable licensing should be offered. It should be possible to take at least 64 snapshots per file system.

16) Proposed storage shall support post process deduplication and compress on SSD tier.

17) The proposed storage array must support data at rest encryption offering industry standard certification/compliance. The storage array may implement data at rest encryption using self-encrypting drives or controller-based functionality there by not impacting performance.

18) The controller should have DE-duplication & compression features for file system access and necessary licensing for the offered solution should be included.

19) It should be possible to configure quotas on the user, volume and directory level.

20) Storage controller shall support NDMP for backup and restore operation.

21) Shall support LDAP and Active Directory integration

xv. **Management Software**

1) The software for managing the storage device should be Web GUI based or CLI.
2) The storage should have out-of-band management feature on Ethernet.
3) Storage administrator console shall be protected by multi-factor authentication
4) The proposed management interface should be able to manage, configure and monitor the environment.
5) Single management, easy to use GUI based and web enabled administration interface for configuration, storage management and performance analysis tools for both block and file.
6) The interface shall allow to manage the entire storage solution from single interface which allows - Storage Management, Cluster Management, DR Configuration Management.
7) The management console shall allow to generate reports on block and file access for a given duration for per node, per user, per volume on a specific administrative domain.
8) On-premise performance analysis, workload planning should be supported

xvi. **Audit Trail Capability.** The Storage solution shall offer suitable solution to retain detailed of NFS Transaction Log to record every file access on the shared file system. The audit log shall include access time stamp, client node IP, mode of access (read or write) and user information. This log shall be retained at least for last 72 hours and shall be in searchable format. Vendor shall offer required resources for capturing this information.

xvii. **Power Requirement.** The offered storage solution should be supplied with hot swappable redundant power supply units, for all the components (Storage Controller, desk Shelves) wherever provision exists in addition to No Single Point of Failure clause mentioned earlier.

1) Power Supply rating: 220 volt/50 Hz.
2) Required power cable shall be offered with the storage.

xviii. **Interfaces / Ports per Controller**

1) Each storage controller should be configured following network ports:
    i. 1G Copper Ethernet - 2 Nos
    ii. 10 G Fiber Ethernet (10 G SR LC Type) – 4 Nos
2) Link aggregation/ trunking of the Ethernet ports should be supported.
3) FC Port – Each storage controller should also be configured with two 16 Gb FC port with transceiver (SR type) for connecting to the SAN switch for backup and for providing block access.

4) Required network cables and FC cables to be offered.

xix. **Performance.** The offered storage controller (each controller) shall support minimum throughput of 50000 IOPS at 8K block size with NFS. Bandwidth – 1.6 GBps with 32 K block size at 80% read and 20% write with NFS.

xx. **Compliance & Certification.** The offered product must be complaint to following certification or equivalent global certification –

1) RoHS India [E-Waste (Management) Rules, 2016] certification Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard
2) Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer/ Hardware.
3) Valid Indian Common Criteria Certification Scheme (IC3S) for EAL2 or better for the offer product or offered version of firmware.

xxi. **POC Requirement**

1) The vendor/OEM shall offer similar storage product in remote access mode over Internet for NSIL to evaluate the features of the offered product during technical evaluation of the offer wherever NSIL request for such POC to the vendor.
2) The offered product for evaluation shall be on offered product line with similar storage operating system version with required licenses.
3) If multiple vendors offer same OEM product on similar BOM, a single remote access offered directly from OEM shall be asked for evaluation of the product
4) NSIL will need access to the storage product for management console and two NFS clients and two SAN client on the network to evaluate the product features.
5) Vendor shall ensure NSIL has remote access to storage controller management console, storage controller logs, client device and logs. NSIL shall evaluate high availability feature, multi-tenancy feature etc. for the product and suitable configuration shall be offered.
6) NSIL will communicate to the Vendor on specific feature sets which NSIL would like to evaluate on the offered product. The selection of the specific product features will be decided by Competent Authority during the technical evaluation process.
7) NSIL will decide the demonstration requirement of feature sets across

OEM products and the requirement will vary based on OEM product.

8) Vendor shall assist NSIL team in configuration and demonstration of product features.

9) Vendor shall keep all the required resource ready for remote evaluation during quoting for this tender. The remote lab configuration diagram, access credentials and access methods shall be shared along with the technical offer. The vendor shall enable remote access immediately after receipt of the email communication via NSIL purchase.

10) In case the vendor or OEM is not able to successful demonstration of the feature with-in two weeks' time after receipt of the requirement, NSIL will not accept any further request for extension or re-evaluation of the feature demonstration activity.

11) The outcome of the feature demonstration will be based on the decision of the NSIL Purchase.

b. Backup Software (host-based license)

i. **Backup Solution Architecture**

1) The backup software should be offered on RHEL platform. Backup Software offered should be compatible with offered RHEL version on Backup Server.

2) Backup/restore software architecture should assure continuity of backup/restore operations even under the failure of one of the nodes involved in the backup/restore (i.e. NAS filer/file server nodes)

3) The backup / restore solution should permit multiple copies of the backups to be maintained including the support for offline vaulting of one or more copies

4) It shall be possible to take tape backups for the following:
   - a file
   - a directory
   - a directory structure
   - an entire volume
   - any snapshot copy

5) The following backup options shall be supported:
   - Full backup
   - Incremental backup
   - Differential Backup

6) The administration facility should be provided using a suitable easy-to-use GUI to centrally monitor and administer the backup environment.

7) It should also be possible to manage & administer backup environment using command line Interface.

8) The backup software should be capable to perform policy based automated backup scheduled based on calendar schedule (specific day, week, month).

9) The backup software should have options to choose the following features:
    - Backup Window
    - Backup Retry
    - Backup Source
    - Backup Media Pool

10) The backup software should have option to take backup of entire backup configuration and catalog data

11) It should be possible to restore the following:
    - Full File System.
    - Selected Directories.
    - Selected file/s

12) Proposed solution must include safeguards against ransomware attacks or intentional deletion of backup data by malicious actors who exploit compromised authentication on the backup server or software. Access to data in recovery scenarios must be restricted to "Recovery Admin" or "Super Admin" roles, and this access should be secured through dedicated local authentication, segmented business user access, or Multi-Factor Authentication (MFA) utilizing SAML or integration with third-party solutions such as OneLogin, Azure, and Okta etc.

13) Proposed backup solution should strengthen the defenses against ransomware and other cyber-attacks with features including: immutable backups, ransomware recovery, object storage locking, cloud tiering with data locking, data encryption, multi-factor authentication, restricted backup storage protocol for Storing all critical backups

ii. **License Requirement**

1) The offered backup solution should have host based NDMP or dual socket license for taking NDMP backup of the NAS storage for full volume without NAS capacity limitations

2) Software shall support both direct and 3 way NDMP Backup.

3) Offered Solution must support Browsable Volume Selection and Direct Access Restore(DAR) for Backups from the Tape to NAS Mount Point, which enables fast recovery of whole directories, single files, or subsets of files by recording each file's location within the backup media and should avoid sequential-read through the entire backup set for faster restoration

4) Offered Solution must support Incremental Restore for specific backup

data

5) Offered Solution must support Dynamic Drive Sharing on SAN Tape Drives between NAS devices (Filers) / Backup Server / SAN Clients and Operate seamlessly between multiple platforms

6) The backup solution should be offered with 2 numbers of network client with single socket count license in Linux platform.

iii. **Backup Management Feature**

1) It should be possible to restore the contents of the media on a system different from the one on which the backup was taken

2) It should provide a user-friendly enterprise console that enables the administrator to manage the complete backup and recovery environment via a Web-based interface

3) The proposed backup solution should allow search capability enables fast and granular searches of its backup index for backup and restore. Include fast-search capabilities for metadata (name, modified date, type, etc.) and save-sets with offline indexes in your search results

4) Backup Solution must have Single sign-on (SSO) features to Log into Backup Software using AD/LDAP credentials along with Role-based access control to regulates operations administrators

c. Tape Library -

i. 19-inch Rack Mountable – 3U/4U Tape library.

ii. The tape library should be configured with two LTO9 tape drives. All the drives must be Dual Port LTO9 FC Drives. The LTO 9 Drive FC interface shall be compatible with offered SAN switch.

iii. The number of slots for tape media should be minimum 40 Slots usable/Licensed, without Stacking modules.

iv. The tape library should support minimum five mail slots.

v. The tape library should be with two or more magazine configuration.

vi. The tape library should support both read and write operations of LTO9 media.

vii. Offered LTO9 drives in the Library shall conform to the Continuous and Data rate matching technique for higher reliability.

viii. Offered Tape Library shall have partitioning support so that each drive can be configured in a separate partition. Required license shall be offered.

ix. The tape library should have a GUI panel & also should be manageable remotely from web-based GUI.

x. It should be possible to manage the following using both local & remote management - Moving media, Load/unload tape drives, Access to the diagnostics, Library configurations, Library statistics, Inventory check.

xi. The tape library native capacity should be minimum 720TB Native and 1.8 PB (compressed 2.5:1). Required license shall be offered.

xii. The tape library transfer rate should be 3.24 TB/Hr (native) in fully loaded configuration (3 Drive configuration).

xiii. MSBF (Mean Swaps Between Failures) >= 1 Million Robot load/unload cycles or MTBF of 125,000 Hours.

xiv. Native Transfer Rate: > = Shall support full throughput from all the drives operating concurrently at their maximum transfer rates.

xv. The Tape Library should have FC interconnect to the SAN switch to enable NDMP backup and restore operations.

xvi. The Tape Library should support taking backup over NDMP.

xvii. The offered tape library should be configured with Field Replaceable Tape Drives, Magazines, Power Supply Units

xviii. The Tape Library should have barcode reader feature for media management. Required number of Barcodes shall be included in the offer.

xix. Proactive Diagnostics: Proactive monitoring feature within the library to monitor major subsystems, run self-diagnostic procedures, and send policy-based communications to system administrators

xx. Support for auto clean feature

xxi. Encryption capability - AES 256-bit

xxii. Dedicated management port for remote management of Library

xxiii. Number of LTO9 Tape Media to be offered = 70

xxiv. Number of cleaning cartridges to be offered =10

xxv. Hot Pluggable redundant power supply, 80 plus rating

xxvi. Regulatory Ratings –

- Safety: IEC-60950 with worldwide country deviations with Class 1 Laser product
- Emissions Standards: FCC Class A or equivalent Indian standard
- ROHS or ROHS India

d. <u>Backup Server</u>

i. **Physical** – 19-ich rack mountable server of 2U rack mount size. Servers shall be offered with required rack mount hardware kit.

ii. **Processor** – single processor with minimum 16 cores and 2.4 Ghz clock or better processor (Intel or AMD).

iii. **Memory** - 96 GB Memory in best deployable model

iv. Internal Storage Hot pluggable HDD: 2 Nos of 1.92 TB Mix Use Hot Pluggable SSD with DWPD >= 1.0 in RAID 1

v. **Drive Bay** – Server shall support 4 Hot-Plug Hard disk drive Bay

vi. The server must be RHEL certified hardware and listed in RHEL portal.

vii. **Drive Controller** – 12G SAS controller with RAID 1.

viii. **Optical Drive** – Internal DVD RW drive to be offered

ix. **Network Controller** – Two 1G Ethernet port and four 10G Ethernet ports

x. **HBA Port** - The server should be configured with two numbers of 16Gb FC HBA cards for connecting to the SAN switch. Vendor should offer multipath driver for HBA

xi. **Ports** – Front :2 USB, Rear: 4 USB, VGA=1

xii. **Power** – Hot Pluggable redundant power supply. Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

xiii. **Management** - Server shall include IPMI 2.0 compliant management module . Management function shall be offered on out of band over Ethernet.

xiv. Management functionalities (viz., power off, power on, reboot, System health monitoring, remote media mount and software installation) should be possible to be carried out using the offered management module.

xv. **Cooling** – Server shall be configured with redundant cooling fans.

xvi. **Certifications** – Following or equivalent international certification
   (a) RoHS India [E-Waste (Management) Rules, 2016] certification
   (b) Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard
   (c) Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

xvii. If the offered backup software requires a better configuration, the required hardware should be offered.

e. <u>SAN Switch</u>

i. Vendor has to offer SAN Switches with the following specifications:

ii. 16 Gb FC ports = 12 nos

iii. Non-blocking wire speed performance for all ports. i.e. minimum 384 Gbps of switch bandwidth

iv. Required FC transceivers should be included.

v. 12 nos of 5 meter FC cables should be offered.

vi. Should be offered with ISL trunking license

vii. Class of service: Class 2, Class 3, and Class F

viii. Supported fabric services - Name server, Registered state change notification (RSCN), Login services, Public loop, Broadcast, In-order delivery, Name-server zoning, NTP.

ix. Supported diagnostics features - Power-on self-test (POST) diagnostics, Online diagnostics, Fiber Channel traceroute capability, Fiber Channel ping and debug, Syslog, Port-level statistics.

x. Should be offered with zoning (default zoning, port/WWN zoning, broadcast zoning) and VSAN licenses.

xi. Supported management features - HTTP, SNMP V1/V3, SSH

xii. Should be configured with dual hot swappable power supply

xiii. Should be configured with adequate cooling fans.

xiv. Should support out of band management over Ethernet.

xv. Should support configuration and management over web console.

xvi. 19 inch rack mountable with rack mount kit.

xvii. Compliance – CB, WEEE, ROHS

f. <u>Installation & Commissioning –</u>

i. Vendor shall provide required FC interconnection cables for integration of SAN switch, Tape Library, Backup Server and Storage.

ii. Vendor shall implement NDMP LAN Free backup and make suitable interconnect and policy configuration.

iii. Vendor shall provide four numbers of 10 meter FC cables for interconnecting NAS 10G ports with LAN switches.

iv. Vendor shall provide required number of FC cables for interconnecting Tape Library, SAN switch and Storage HBA ports during installation.

v. Vendor should provide detailed documentation on storage solution acceptance and implementation as a part of solution implementation activity.

vi. Vendor shall depute certified engineer on Storage and backup environment to carry out the acceptance and implementation at Bhopal.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'D' - RACK Servers

Specifications for Rack Server – Configuration – 1:

a. **Physical** – 19-inch rack mountable server of 1U rack mount size. Servers shall be offered with required rack mount hardware kit.

b. **Processor** – One Intel® Xeon® Gold 6548N Processor (60M cache, 32 Cores, 64 Threads, 2.80 GHz) or better or equivalent AMD processor on X86-64 architecture.

c. **Memory** - 128 GB ECC memory spread across all memory channels or better memory configuration.

d. **Internal Storage** – 6 Nos of 1.92TB SAS 12G Mixed Use SFF SSD Drive Writes Per Day (DWPD) > = 1

e. **Drive Controller** – Internal RAID Card for RAID 1, 0, 10, 5 and 6 support with 8 GB Memory

f. **OS Certification** - RHEL & Windows certified hardware. All the required device drivers for RHEL shall be included in the offer. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

g. **Optical Drive** – Internal DVD RW drive to be offered

h. **Network Controller** – Total 4 nos of 1Gb Ethernet copper and four numbers of 10Gb Ethernet Copper port shall be configured for each server.

i. **Ports** – Front :2 USB, Rear: 4 USB, VGA=1

j. **Power** –Hot Pluggable redundant power supply. Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

k. **Management** - Server shall include IPMI 2.0 compliant management module . Management function shall be offered on out of band over Ethernet.

l. **Cooling** – Server shall be configured with redundant cooling fans.

m. **Certifications** – Following or equivalent international certification

- RoHS India [E-Waste (Management) Rules, 2016] certification
- Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard
- Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer
- Security Compliance – TPM 2.0, UEFI Secure boot

q. **Support for Proxmox VE** – The offered server platform shall be compatible with Proxmox VE HCI solution. If the solution is not compatible to Proxmox, then vendor need to quote for equivalent HCI license for 3 clusters each with minimum 3 node

and each Cluster shall host 10 VMs. The CPU core, disk and memory support shall be as per offered server configuration. The HCI platform shall have OEM support during the support period for upgrade and bug fixes. The vendor also need to ensure implementation of the cluster as per implementation requirement described in the subsequent section.

r. **Operating System**– **RedHat Enterprise Linux 9.x or latest:** EIGHT nos of 2 socket licenses with 7 years support to be provided.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'E' – Edge Switches

Specifications for Edge Switch (Mission) (24 Port):

a. **Physical.** 19-inch rack mountable chassis along with rack mount kit. Offered switch shall be within 2U form factor.

b. **Port Requirement:**

   i. Switch shall have at least 24 nos. of 10/100/1000 Base-T ports and additionally at least 4 nos. of 1/10 Gbps SFP Gbps SFP+ uplink ports (SX/LX).

   ii. The Switch shall be configured with 2 nos. of 1000 BaseLX transceivers (out of the four combo ports mentioned above) to support minimum upto 10 KM.

   iii. The transceivers offered should be from the same switch manufacturer (OEM) only.

   iv. Switch should have dedicated slot for modular stacking, in addition to asked uplink ports.

   v. Required stacking cable (3 Meter) shall be delivered with each switch

c. **Scalability requirement.** Offered switch should capable to support a future upgrade to 2 * 25Gbps uplink module.

d. **Performance**

   i. Minimum Switching capacity 148 Gbps (Excluding Stacking Bandwidth)

   ii. Minimum Throughput 110 million pps (Excluding Stacking Bandwidth)

   iii. Offered switch shall be fully non-blocking architecture

   iv. The configuration for an individual switch shall be realized using a single chassis (not by stacking)

e. **General Feature –**

   i. **Trunking**: Maximum ports per trunk: 8, Maximum trunk groups: 4

   ii. The offered switches shall be hardware ready for SDN support

   iii. Support for PTP and NTP

   iv. Switch shall offer open flow V1.0/V1.3 or equivalent.

f. **Layer 2 Features –**

   i. VLAN support and tagging

ii. 802.1s Multiple Spanning Tree Protocol

iii. 802.1X Authentication

iv. MAC-Layer Filtering

v. Port Security - MAC Learning Disable

vi. Jumbo packet support, Max Size=9000 Bytes

vii. Rapid Per-VLAN Spanning Tree (RPVST+)

g. **Layer -3 Features –**

i. VRF / VRF-lite

ii. BGP, OSPF and IS-IS Routing

iii. VRRP/VRRP-E/HSRP

iv. Multicast Routing

v. Generic Routing Encapsulation (GRE)

vi. Switch should support minimum 16 VRF instances with route leaking functionality

vii. Switch should be able to support sub-interfaces

viii. Switch should support open standards based EVPN to support VXLAN based overlay network for layer-2 (VLAN) and layer-3 (VRF) extension.

ix. The Switch should support 10k IPv4 LPM (Longest Prefix Match) routes

x. Support for port mirroring on L3 network

xi. Static and Dynamic NAT

h. **IPV6 Support –**

i. IPv6 host support at the edge network

ii. IPv6 Routing (OSPF v3),BGP4+ (IPv6)

iii. VRF (IPv6)

iv. IPv6 over IPv4 tunnels

v. Multicast Listener Discovery (MLD) version 2 snooping

i. **Security Features –**

i. 802.1x Accounting

ii. MAC Authentication

iii. Protection against Denial of Service (DoS) attacks

iv. Encryption -- Must support 128-bit Advanced Encryption Standard (AES) for SSL/Management encrypted traffic

v. ACL - Provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number

vi. MACSEC

j. **Supported Protocol and RFC Standards-**

i. 802.1D Bridging

ii. 802.1q VLAN Tagging

iii. 802.1p Mapping to Priority Queue

iv. 802.1w Rapid Spanning Tree (RSTP)

v. 802.3ad Link Aggregation

vi. 802.3x Flow Control

vii. SNMP V1, V2, V3

viii. RFC 783 TFTP

ix. RFC 854 Telnet

x. RFC 1757 RMON MIB

xi. RFC 896 Congestion Control in IP/TCP Internetworks

xii. RFC 950 Internet Standard Sub-netting Procedure

xiii. RFC 1191 Path MTU Discovery

xiv. RFC 1403 BGP OSPF Interaction

xv. RFC 1519 Classless Inter-Domain Routing (CIDR):

xvi. RFC 1812 Requirements for IP Version 4 Routers

xvii. RFC 2236 Internet Group Management Protocol (IGMP) Version 2

xviii. RFC 1887 An Architecture for IPv6 Unicast Address Allocation

xix. RFC 1981 Path MTU Discovery for IPv6

xx. RFC 2374 IPv6 Aggregatable Global Unicast Address Format

xxi. RFC 2373 IPv6 Addressing Architecture

xxii. RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)

xxiii. RFC 5308 Routing IPv6 with IS-IS

xxiv. RFC 7348- Virtual extensible Local Area Network (VxLAN)

xxv. RFC 1349 Use of OSI IS-IS for routing in TCP/IP and dual environments

xxvi. OEM can refer to updated or equivalent RFC wherever applicable

k. **Power Supply**

i. Switch shall be configured with Redundant hot-swappable internal power supplies

ii. Switch shall be configured with Hot-swappable fan assembly

iii. Power Supply: Should be offered with two internal, redundant, field-replaceable, hot-swappable AC power supplies (100 to 240 VAC, 50 to 60 Hz)

iv. All the switches shall be delivered with required power cables with C13 PDU cables with suitable length (3 Ft or 5 Ft).

l. **Switch Management**

i. Command-line interface

ii. Out-of-band management (RJ-45 Ethernet and serial RS-232C/Micro USB)

iii. SNMP Manager

iv. Console cable to be included with each switch

v. The proposed switch should have enough Memory (Flash and RAM) to hold the latest Software Release. Switch should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc.

vi. Switch should support for execution of script for device management for automatic and scheduled system status update for monitoring and management

m. **Reliability**

i. Switch shall have MTBF 150,000 Hours or better. Vendor shall provide required datasheet or OEM certification to establish MTBF of the offered hardware.

ii. Components, like modules/ power supplies/ fan tray should be Hot Swappable. Online insertion and removal (OIR) support is must for modules, Power supply and FAN.

iii. Switch should support for (Bidirectional Forwarding Detection) BFD for Multipoint network for fast Failure Detection as per RFC 5881 or equivalent

n. **Environmental regulatory compliance.** Following or equivalent international certifications

i. RoHS India [E-Waste (Management) Rules, 2016] certification

Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

ii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer/ Hardware

iii. Security Compliance – OEM signed image verification

iv. Valid Indian Common Criteria Certification Scheme (IC3S) for EAL2 or better for the offer product or offered version of firmware

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'F' – Core Switch

Specifications for Core Switch

a. **Physical.** 19-inch rack mountable chassis along with rack mount kit.

b. **Chassis.**

i. Switch should not be configured with any over-subscribed line interface cards.

ii. The configuration for an individual switch shall be realized using a single chassis.

iii. The offered chassis should not have any active components in unloaded condition (bare chassis without any line cards and power supplies)

c. **Fabric**

i. The Switch should provide a non-blocking, distributed switching fabric architecture

ii. Management functionality should be available with full redundancy

iii. In case, the management functionality is integrated with a line card, then redundancy shall be provided by duplicating that card or by an alternate card supporting management functionality

iv. Failure of any supervisor engine or fabric module should not bring down the performance, redundant components needs to be proposed accordingly.

v. Switch fabric to be provided with redundant switch fabric capability

vi. The architecture of the switching fabric should be modular & Hot Pluggable

d. **Port Requirement – Each Switch shall be configured with**

i. 1/10 G Ethernet Port = 96 Nos, Can be offered with 40 Nos 1G Copper and 56 Nos 10G Coper interface native or with Transceiver with suitable line card arrangement if 1/10G native Copper Interface line cards are not available

ii. 1/10/25 G Fiber - 48 No

iii. 40/100 Gbps QSFP uplink ports (SR/LR) = 4 Nos. 40/100G ports Shall be offered through two or more independent line cards

iv. Each switch shall have following transceivers loaded
1) 1G (SX) SFP LC = 10 Nos
2) 1G (LX) SFP LC (Upto 10 KM)= 8 Nos

3) 10G (LR)SFP+ LC (Upto 10 KM) = 8 Nos
4) 10G (SR)SFP+ LC = 8 Nos
5) 25G (SR) SFP28 LC = 4 Nos
6) 40G (SR) BiDi QSFP+ LC = 4 Nos

v. The transceivers offered should be from the same switch manufacturer (OEM) only

e. **Performance-**

i. Per slot minimum 6.0 Tbps bandwidth.

ii. Latency - The Switch should have capability to support latency as low as 3.98 microsec for packet size of 64-Bytes.

iii. The offer chassis shall be capable to support 100G ports 30 Nos in single line card in non-blocking mode in all payload slot of the chassis

iv. The Switch should have a Truly Distributed Architecture. All Interface Modules should have all the resources for switching and Routing and should offer True Local Switching (Intra-Module and Inter-Module).

v. Switch should support minimum 128 VRF instances with route leaking functionality

vi. The Switch should support 350k IPv4 LPM routes

vii. The line card proposed in the Switch should have minimum 32MB packet buffer and it should support minimum of 64MB of buffer on 100 Gig line Cards.

viii. The Switch should support 100k multicast routes

ix. Switch platform should support MAC Sec (802.1AE) in hardware for 100G ports.

f. **SDN Feature.** The offered switches shall be hardware ready for SDN support.

g. **Layer 2 Features –**

i. VLAN support and tagging (IEEE 802.1q)

ii. Spanning Tree Protocol (IEEE 802.1D, 802.1W,802.1S)

iii. MAC Address Locking and MAC layer Filtering

iv. MAC Address Locking and MAC layer Filtering

v. IGMP v2

vi. PIM-SM Snooping, Support Multicast Source Discovery Protocol (MSDP) - RFC 3618

vii. Jumbo packet support, Max Size=9000 Bytes

viii. Rapid Per-VLAN Spanning Tree (RPVST+)/ RSTP or equivalent

h. **Layer -3 Features –**

i. VRF/ VRF Lite

ii. VRF Leaking

iii. BGP RFC 4271

iv. OSPF and IS-IS

v. VRRP/ VRRP-E / HSRP

vi. RIP v2

vii. Multicast Routing RFC 2858 or equivalent

viii. Generic Routing Encapsulation (GRE)

i. **IPV6 Support –**

i. IPv6 Routing (OSPF v3), BGP4+ (IPv6)

ii. OSPF for IPv6

iii. VRRP-E (IPv6)/ HSRP(IPv6)/VRRPv3

iv. VRF (IPv6)

v. IPv6 over IPv4 tunnels

vi. Multicast Listener Discovery (MLD) version 2 snooping

j. **Security Features –**

i. MAC Authentication

ii. Protection against Denial of Service (DoS) attacks

iii. Encryption -- Must support 128-bit Advanced Encryption Standard (AES) for SSL/Management encrypted traffic

iv. ACL - Provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number

v. Must support switch-port configuration to block flooding of unknown multicast or unicast traffic.

vi. Must support traffic storm control to monitor the levels of the incoming broadcast, multicast, and unicast traffic against a set threshold and filter out subsequent packets when a threshold is reached.

vii. TPM 2.0 or Secure boot or should support image verification with OEM signed certificates

viii. Time based ACL or Equivalent

k. **Supported Protocol and RFC Standards-**

i. 802.1D Bridging

ii. 802.1q VLAN Tagging

iii. 802.1p Mapping to Priority Queue

iv. 802.1w Rapid Spanning Tree (RSTP)

v. 802.3ad Link Aggregation

vi. 802.3x Flow Control / Priority-based flow control (PFC) - 802.1Qbb

vii. SNMP V1, V2, V3

viii. RFC 950 Internet Standard Subnetting Procedure

ix. RFC 1403 BGP OSPF Interaction or should support route exchange between protocols

x. RFC 4632 Classless Inter-Domain Routing (CIDR)

xi. RFC 4604 Internet Group Management Protocol (IGMP) Version 3

xii. RFC 4291 IPv6 Addressing Architecture

xiii. RFC 1981 Path MTU Discovery for IPv6

xiv. RFC 4193 / RFC3587 Unique Local IPv6 Unicast Addresses

xv. RFC 6241 Network Configuration Protocol (NETCONF)

xvi. RFC 4861 or equivalent for Neighbor Discovery for IP Version 6 (IPv6)

xvii. RFC 3623 Graceful OSPF Restart

xviii. RFC 5308 Routing IPv6 with IS-IS

xix. RFC 1195 Use of IS-IS for Routing in TCP/IP and dual environment

xx. OEM can refer to updated or equivalent RFC wherever applicable

l. **Virtualization Features (VPC or VCS)**

i. VXLAN (RFC 7348)

ii. VX LAN Routing, VXLAN Bridging , VRF aware VXLAN Routing / Multi tenancy

iii. Switch should support layer 2 extension over VXLAN (RFC7348) across all DataCenter to enable VM mobility & availability

iv. Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890

m. **Reliability and Availability**

i. The Switches should have hardware level redundancy in terms of data plane and control plane. Issues with any of the plane should not impact the functioning of the switch

ii. Chassis shall have MTBF 450,000 Hours or better. Vendor shall provide required datasheet, certification or a signed legal letter to establish MTBF of the offered chassis.

iii. There should not be any single point of failure in the switch. All the main components like CPU module, switching fabric, support module, system clock, power supplies and fans etc should be in redundant configuration.

iv. Components, like modules/ power supplies/ fan tray should be Hot Swappable. Online insertion and removal (OIR) support is must for modules, Power supply and FAN.

v. Module replacement should not require rebooting of the switch or create disruption in the working of the switch.

vi. Switch should support for (Bidirectional Forwarding Detection) BFD for Multipoint network for fast Failure Detection as per RFC 5881 or equivalent RFC

vii. The chassis should Support Dual Supervisor based In service Software Upgrade (IISU)/ Graceful Routing Engine Switchover (GRES) with NonStopForwarding/equivalent

viii. There should not be any impact on the performance in the event of the software upgrade/downgrade.

n. **Power Supply –**

i. The switch should be offered with hot swappable redundant Power Supply Units with N+N configuration

ii. The offered power supply must meet 80 Plus Silver or better power efficiency. For make in India products as per Bureau of Energy Efficiency, Govt of India Guideline for Computer the compliance shall be submitted.

iii. The offered power supply units should be able to drive the switch in fully loaded configuration with full redundancy

iv. The power supplies shall be rated for 230 V, 50 Hz operation.

v. Matching type of power cables shall be offered with each switch to connect to panel

o. **Cooling**

i. The switch should be offered with hot swappable redundant cooling fans loaded in each chassis

ii. The blowing of air shall be front to rear flow. Side blowing configuration shall not be accepted.

iii. The cooling fans shall be loaded to the full capacity of the chassis

p. **Switch Management –**

i. Device can be managed by command-line interface by SSH; out-of-band management (RJ-45 Ethernet); SNMP Manager; Telnet and FTP; out-of-band management (serial RS-232C or Micro USB)

ii. In case, the management functionality is integrated with a line card, then redundancy shall be provided by duplicating that card or by an alternate card supporting management functionality

iii. Management function shall be state synchronized in active-active or active-standby mode through redundant supervisory cards.

iv. The proposed switch should have enough Memory (Flash and RAM) to hold the latest Software Release. Switch should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc.

v. Switch should support for execution of script for device management for automatic and scheduled system status update for monitoring and management

q. **Environmental regulatory compliance and Certification.** The offered switch must have following certification or equivalent international certification:

i. RoHS India [E-Waste (Management) Rules, 2016] certification Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

ii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer/ Hardware

iii. Security Compliance – TPM 2.0 or Secure boot or should support image verification with OEM signed certificates

iv. Valid Indian Common Criteria Certification Scheme (IC3S) for EAL2 or better for the offer product or offered version of firmware

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'G' – Network Security Appliance

Specifications for Network Security Appliance:

The Network Security Appliance required for the operational Network to include the following devices under single OEM make. Bidder may note that the reference to a specific OEM hardware model is only to define capability and sizing of the product and not to restrict brand. Bidder may offer any OEM product which has same technical capability as mentioned in the RFP. Following devices are required:

No	Device
a.	UTM/Next Generation Firewall (NGFW) – Config 1 & 2
b.	Next Generation Firewall (NGFW) Logger & Traffic Analyser
c.	Next Generation Firewall (NGFW) Manager
d.	UTM Hardware Authentication Token
e.	End Point Protection & Management Capability

a. **UTM/Next Generation Firewall (NGFW) - Config-1**

i. **Specification**- Next generation Firewall with integrated IPS, IDS, Antivirus and Gateway-antivirus, as per detailed specifications below. Vendor can quote products equivalent or better to Fortigate 121G (Part No. FG-121G) with Unified Threat protection.

ii. **Physical and General Specification –**

1) 19-inch rack mountable chassis along with rack mount kit. Offered device shall be with-in 2U form factor.
2) The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened proprietary operating system. The firewall appliance should support Integrated IPS, IDS, DLP, DoS, Web-Filtering, Antivirus and Application control feature.
3) The firewall appliance should support dual stack IPv4 and IPv6
4) The proposed solution should support dynamic routing like RIP1, RIP2, OSPF, BGP4.
5) Device shall support for upto 10 nos of firewall virtual partitioning. Each partition/instance should act as independent firewall with all features and should have independent users and resource management capabilities.
6) The UTM/NGFW shall have provision for integration with centralized management and definition update by specialized firewall manager device. The centralized manager will be form the same OEM of offered UTM/NGFW make.
7) The UTM/NGFW shall have centralized logging and report generation device by same OEM make as a specialized hardware for traffic report generation.

iii. **Port Requirement –**

1) The UTM/NGFW shall be offered with 1G RJ45=16 Nos, 1G Fiber=8 Nos, 10G Fiber=4 Nos with 02 Nos of 10GE SFP+ and 08 Nos 1G single mode LC SFP transceivers (Upto 2 KM),

2) The transceivers offered should be from the same OEM or OEM Certified.

iv. **General Features –**

1) The NGFW shall have Storage: 480 GB SSD internal storage.
2) Firmware should reside on Internal Flash.
3) The internal SSD and Firmware Flash shall be removed and retained with User during a device replacement or during any failure in SSD or Flash.
4) The proposed solution should have unrestricted user/node license.
5) The proposed solution must support user based policy configuration for security & management.
6) The proposed solution should support Route (Layer 3), transparent mode (Layer 2) and MIX mode deployment.

v. **Performance –**

1) The offered NGFW shall have following performance figures for Enterprise traffic mix - Firewall: 28 Gbps (with 64 Byte UDP Packet), IPS: 5.3 Gbps, NGFW:3.1 Gbps, Threat Protection Throughput 2.8 Gbps, Firewall Latency: 3.17 microsecond (for 64 Byes UDP packet) or better
2) Device shall support minimum 2000 Nos of IPSec Site-to-Site VPN
3) The configuration for an individual Firewall shall be realized using a single chassis (not by stacking).

vi. **Administration, Authentication & General Configuration Feature –**

1) The proposed solution should support administration via secured communication over HTTPS, SSH and from Console.
2) The proposed solution should be able to export and import configuration backup including user objects.
3) The proposed solution should support user/ip/mac binding functionality to map username with IP address & MAC address for security reason.

vii. **IPV6 Support –**

1) IPv6 Routing
2) IPv6 Multicast Routing
3) IPv6 over IPv4 tunnels

viii. **High Availability Features –**

1) The proposed solution should support High Availability Active/Passive or Active/Active deployment. The license shall be offered along with the product
2) The proposed solution should support Link, device & Session failure.
3) The proposed solution should support automatic & manual synchronization between appliances in cluster

ix. **Power Supply –**

1) Should be offered with internal, redundant power supplies (220 VAC at 50 Hz)
2) Required number of power cables (IEC-13/14 Power Cord 2 Meter) shall be offered with each device

x. Firewall Management command-line interface; Web browser; out-of-band management (RJ-45 Ethernet); SNMP Manage; out-of-band management (serial RS-232C or Micro USB)

xi. **Environmental regulatory compliance**

1) RoHS-compliant / RoHS India
2) FCC and CE norm or equivalent as per Govt. of India guideline

xii. **Product Certification Security Certification -** Valid Indian Common Criteria Certification Scheme (IC3S) for EAL4 or equivalent certification for the offered device or firmware.

b. **UTM/ Next Generation Firewall (NGFW) - Config-2**

i. **Specification-** Next generation Firewall with integrated IPS, IDS, Antivirus and Gateway-antivirus, as per detailed specifications below. Vendor can quote products equivalent or better to Fortigate 91G(Part No. FG-91G) with Unified Threat protection.

ii. **Physical and General Specification**

1) 19 inch rack mountable chassis along with rack mount kit. Offered device shall be with-in 2U form factor.
2) The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened proprietary operating system. The firewall appliance should support Integrated IPS, IDS, DLP, DoS, Web-Filtering, Antivirus and Application control feature.
3) The firewall appliance should support dual stack IPv4 and IPv6
4) The proposed solution should support dynamic routing like RIP1, RIP2, OSPF, BGP4.
5) Device shall support for upto 10 nos of firewall virtual partitioning. Each partition/instance should act as independent firewall with all features and should have independent users and resource management capabilities.
6) The UTM/NGFW shall have provision for integration with centralized management and definition update by specialized firewall manager device. The centralized manager will be form the same OEM of offered UTM/NGFW make.
7) The UTM/NGFW shall have centralized logging and report generation device by same OEM make as a specialized hardware for traffic report generation.

iii. **Port Requirement**

1) The UTM/NGFW shall be offered with 1G RJ45=8 Nos, , 1G/10G Fiber= Nos with 02 Nos of 1G single mode LC SFP transceivers (Upto 2 KM).
2) The transceivers offered should be from the same OEM or OEM Certified.

iv. **General Features**

1) The NGFW shall have Storage: 120 GB SSD internal storage.
2) Firmware should reside on Internal Flash.
3) The internal SSD and Firmware Flash shall be removed and retained with User during a device replacement or during any failure in SSD or Flash.
4) The proposed solution should have unrestricted user/node license.
5) The proposed solution must support user based policy configuration for security & management.
6) The proposed solution should support Route (Layer 3), transparent mode (Layer 2) and MIX mode deployment.

v. **Performance**

1) The offered NGFW shall have following performance figures for Enterprise traffic mix - Firewall: 27 Gbps (with 64 Byte UDP Packet), IPS: 4.5 Gbps, NGFW:2.5 Gbps, Threat Protection Throughput 2.2 Gbps, Firewall Latency: 3.23 microsecond (for 64 Byes UDP packet) or better
2) Device shall support minimum 2000 Nos of IPSec Site-to-Site VPN

3) The configuration for an individual Firewall shall be realized using a single chassis (not by stacking).

vi. **Administration, Authentication & General Configuration Feature**

1) The proposed solution should support administration via secured communication over HTTPS, SSH and from Console.
2) The proposed solution should be able to export and import configuration backup including user objects.
3) The proposed solution should support user/ip/mac binding functionality to map username with IP address & MAC address for security reason.

vii. **IPV6 Support –**

1) IPv6 Routing
2) IPv6 Multicast Routing
3) IPv6 over IPv4 tunnels

viii. **High Availability Features –**

1) The proposed solution should support High Availability Active/Passive or Active/Active deployment. The license shall be offered along with the product
2) The proposed solution should support Link, device & Session failure.
3) The proposed solution should support automatic & manual synchronization between appliances in cluster.

ix. **Power Supply**

1) Should be offered with redundant power supplies (220 VAC at 50 Hz)
2) Required number of power cables (IEC-13/14 Power Cord 2 Meter) shall be offered with each device

x. Firewall Management command-line interface; Web browser; out-of-band management (RJ-45 Ethernet); SNMP Manage; out-of-band management (serial RS-232C or Micro USB)

xi. **Environmental regulatory compliance –**

1) RoHS-compliant / RoHS India
2) FCC and CE norm or equivalent as per Govt. of India guideline

xii. **Product Certification Security Certification -** Valid Indian Common Criteria Certification Scheme (IC3S) for EAL4 or equivalent certification for the offered device or firmware.

c. **Next Generation Firewall (NGFW) Logger and Traffic Analyzer**

i. **Specification-** Vendor can quote products equivalent or better to Fortigate FAZ-1000G (Part No.FAZ-1000G). The NGFW logger and Traffic Analyzer shall be a same OEM make specialized device or appliance as the offered NGFW.

ii. **Physical and General Specification –**

1) The firewall logger device shall be a dedicated appliance based device with 24TB Storage capacity (with RAID protection) for logging the firewall logs, 4 x 1GbE RJ45 Network Interface, 2x 1GbE SFP Interface, and up to 660 GB/Day of Logs.
2) The logger shall have capability to partition the Logger to have dedicated Logging instance from different network segments with-out mixing traffic from other segment.

3) The failed disks shall not be returned back during warranty support.
4) The logger shall have advance analytics capacity and shall also work as a SOC for UTM traffic
5) The device shall show traffic log, event log, DNS log, security logs etc in different category
6) The device shall support custom and automated report generation and shall integrate with Email
7) Device shall have hot swappable redundant power supply.
8) Device shall support TPM 2.0

d. **Next Generation Firewall (NGFW) Manager**

i. **Specification-** Vendor can quote products equivalent to Fortigate FMG-200G(Part No. FMG-200G). . The NGFW Manager shall be a same OEM make specialized device or appliance as the offered NGFW.

ii. **Physical and General Specification –**

1) The firewall manager device shall be a dedicated appliance based device.
2) The product shall support 30 Devices/UTM partitions
3) Device shall be 1 U Rack Mount
4) Device shall have 4 Nos of 1G interfaces
5) Device shall support TPM 2.0
6) Storage Capacity 4TB with RAID protection
7) Device shall have hot swappable redundant power supply configured.

e. **Hardware Authentication Token**

i. **Specification-** Vendor can quote products equivalent to Fortitoken 210. The Token shall be a same OEM make specialized device or appliance as the offered NGFW.

ii. **Physical and General Specification –**

1) The physical token shall be TOTP complaint
2) The device shall be tamper resistant/ tamper evident package.
3) Device shall have minimum 3 years life time.
4) The device shall have Lithium non chargeable internal battery.
5) Device shall be Water Resistance IP-65 certified.
6) Device shall be delivered with suitable key seeding option so that keys can be migrated from failed hardware to new hardware. If such feature is not offered, during every RMA OEM to provide key seeding feature.

f. **End Point Protection & Management Capability**

i. **Specification-** Vendor can quote products equivalent to Fortigate Central Management Tool Endpoint Management System (EMS) and Forticlient End Point Protection and ATP Services with managed services. All the elements shall be deliverable from the same NGFW make and integrated in a single fabric.

ii. **Physical and General Specification –**

1) The Central Management Tool Endpoint Management System shall be a KVM deployable VM.
2) The offered end point protection product shall be enterprise class software with device control, application control and anti-malware feature.
3) The end point control software shall be certified for windows and Linux platform.
4) The solution shall provide security fabric integration with manager and logger device
5) The solution shall provide compliance and ATP for client nodes
6) The EMS license shall provide Provisioning, Compliance and Security Fabric, Remote Control, Telemetry and Monitoring feature for the end points.

g. **POC Requirement for NGFW UTM and associated Components** During evaluation process NSIL may need to conduct POC for the offered NGFW and associated products (Manager, analyzer, Client and compliance node) to evaluate the offered product capability. NSIL purchase shall intimate vendor to arrange for required infrastructure on physical or VM infrastructure to carry out feature evaluation of the products and verification of the integration of the components. Vendor has to offered the required infrastructure within two weeks after receipt of the POC requirement. NSIL will need remote access to the infrastructure for carrying out the evaluation.

h. **Hardware Upgrade:** For Item supplied as part of Network Security Appliance, during the support period offered, the offered hardware does not support OEM supported firmware due to hardware obsolesces, vendor needs to provision supported hardware of equivalent configuration and migrate the services in new platform.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'H' – Interconnection Router

a. **Specification for Interconnection Router Config- 1 as follows for per router -**

i. C8300-1N1S-6T Cisco Catalyst C8300-1N1S-6T Router - 1 No

ii. CON-SNT-C830IN6T SNTC-8X5XNBD Cisco Catalyst C8300 - As per support duration

iii. MEM-C8300-8GB Cisco Catalyst 8300 Edge 8GB memory - 1 No

iv. M2USB-16G Cisco Catalyst 8000 Edge M.2 USB 16GB - 1 No

v. C-RFID-1R Cisco Catalyst 8000 Edge RFID - 1RU - 1 No

vi. C8300-RM-19-1R Cisco Catalyst 8300 Rack mount kit - 19" 1R - 1 No

vii. C8300-PIM-BLANK Cisco Catalyst 8300 Edge PIM Blank - 1 No

viii. NETWORK-PNP-LIC Network Plug-n-Play Connect for zero-touch device deployment - 1 No

ix. IOSXE-AUTO-MODE IOS XE Autonomous boot up mode for Unified image - 1 No

x. SC8KBEUK9-173 UNIVERSAL - 1 No

xi. PWR-CC1-400WAC Cisco C8300 1RU AC Power supply - 2 Nos

xii. CAB-IND AC Power Cord (India) - 2 Nos

xiii. NIM-ES2-4 4-port Layer 2 GE Switch Network Interface Module - 2 No

xiv. C-SM-NIM-ADPT Cisco Catalyst SM to NIM Module Adaptor - 2 No

xv. GLC-LH-SMD= 1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM - 2 Nos

xvi. Console Cable – 1 No

P1: The routers must include the Cisco DNA advantage license with full L3 capability. The part numbers listed above is for providing the description of the capability required.

P2: Vendor may note that the part number of Cisco is subject to change. These part numbers are mentioned as indicative. Vendor needs to select the latest part number and equivalent or better feature and offer the complete BOM.

P3. Vendor may also offer router of different make/OEM but with all equivalent physical characteristics and logical features. In such case, vendor may provide a mapping document to show how the features are offered in different make.

b. **Specification for Interconnection Router Config- 2 as follows for per router -**

i. C1121X-8P ISR 1100 8P Dual GE SFP WAN 8GB Router- 1 No

ii. CON-SNT-C1121X8P SNTC-8X5XNBD ISR 1100 8P Dual GE SFP WAN 8GB Router- (As per support duration)

iii. PWR-66W-AC-V2 - Power Supply 66 Watt AC V2 for C890 and C1100 series – 1 No

iv. SL-1K-8P-IPB IP Base License for Cisco ISR 1120 and 1160 8 Ports Series – 1 No

v. CAB-IND - AC Power Cord (India) – 1 No

vi. ACS-1100-RM2-19- Cisco 1100 Series Router Rackmount Kit – 1 No

vii. SISR1100UK9-176 Cisco ISR1100 Series IOS XE – UNIVERSAL – 1 No

viii. L-DNA-TIER-ADD Cisco DNA Subscription License for Routing and SD-WAN – 1 No

ix. C1100-8P-DNA-PF - ISR1100 8-Port Platform Selection for DNA – 1 No

x. IOSXE-AUTO-MODE-PF IOS XE Autonomous or SD-Routing mode for Unified image – 1 No

xi. DNA-P-T0-A-5Y - Cisco DNA Advantage On-Prem Lic 5Y - upto 25M (Aggr, 50M) – 1 No

xii. SL-1100-8P-NA-A-L Cisco ISR1100 8 Port Network Stack Advantage Lic – 1No

xiii. Console Cable – 1 No

P1: The routers must include the Cisco DNA advantage license with full L3 capability. The part numbers listed above is for providing the description of the capability required.

P2: Vendor may note that the part number of Cisco is subject to change. These part numbers are mentioned as indicative. Vendor needs to select the latest part number and equivalent feature and offer the complete BOM.

P3. Vendor may also offer router of different make/OEM but with all equivalent physical characteristics and logical features. In such case, vendor may provide a mapping document to show how the features are offered in different make.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'I' – Server Room Structured Cabling and Accessories

a. **LAN Cables & Accessories and Structured Cabling**

Quantity – The Following LAN cables needs to be delivered. The make of the LAN cable shall be Legrand, Molex, CommScope, AMP, 3C3 or equivalent quality:

No.	Item Description	(Nos.)
1.	1G Ethernet 3 Meter (Color - Green)	200
2.	1G Ethernet 3 Meter (Color - Yellow)	200
3	1G Ethernet 5 Meter (Color - Gray)	150
4.	1G Ethernet 10 Meter (Color - Red)	50
5.	1G Ethernet 15 Meter (Color - Blue)	40
6.	10G Ethernet 3 Meter (Color - Blue)	100
7	10G Ethernet 5 Meter (Color - Reg)	50

General Specification - The offered CAT6 cables should comply the following Standards/certifications:

i. Performance Characteristics – As per ISO/IEC 11801 2nd Edition or better

ii. Fire/Flame Rating – As per IEC 60332-1 or better

b. **Power Cables (Brands --- Legrand, ABB or equivalent quality)**

i. Cable Type-1: Industrial Standard Power Cord with IEC-13 and IEC-14 Connector on either side, 2M/6inch =250 Nos.

ii. Cable Type-2: Industrial Standard Power Cord with IEC-19 and IEC-20 Connector on either side, 2M/6inch=50 Nos.

NOTE: Any additional power/LAN cables required to connect components that are in the scope of this tender to be provided by the vendor at no additional cost.

c. **Rack to Rack Structured Cabling for 10G Ethernet**

i. There are six server Racks and six network racks which are placed facing to each other with a gap as shown in diagram. They are positioned in user server room. Each server Rack has to be provisioned with two CAT6A 24 port fully loaded patch panel. These patch panels needs to be mounted on the rear end of the rack. Thus total of 12 nos of CAT6A 24 port fully loaded

patch panel will be installed for 10G I/O ports (considering six server racks). Each patch panel on server rack side shall have other end terminated on the central network Rack (Network Rack 3 and Network Rack 4) respectively as shown in diagram. Structured Cabling work is required at Bhopal for 10G I/O ports.

ii. Similarly, there will be requirement for 24 Port patch panel (Cat -6A) – between Network Rack 1 to Network Rack 3 and Network Rack 4 to Network Rack 6.

iii. The following table shows the total cable requirement for patch panels.

Description	Reqd. cable length (mt)	Ports/ patch panel	No.of patch panels	No of CAT - 6A IO	No of data point for termination	No.of Racks	Total Cable Length (mt)
Server rack to Network rack	10	24	2	576	288	6	2880
Network rack to Network Rack	5	24	2	96	48	---	240
*Aggregated 4-pair CAT6A UTP cable required for patch panels							3120

iii. Vendor must note that there may be 10% variation in estimation. Vendor must include the cost considering the variation in cable length and make the commercial offer.

iv. Vendor shall use Legrand, Molex, CommScope, AMP, 3C3 or equivalent quality

v. Vendor shall install the data points and certify the Cat6A LAN certifier device.
The following is the scope of data point installation

1) Data Points mentioned in the RFP mean end-to end point installation
2) Laying of 4-pair, Cat 6A UTP Cable through PVC conduit Pipes/Casing. Required conduit pipe and casing must be included in the offer
3) Fixing and Termination of Information outlets and patch panel
4) Labeling of the patch panels, UTP cables for proper tractability and mapping of the ports
5) Dressing of Cables, with Proper end-to-end labelling of cables with ferules and each data-point.
6) Documentation and Testing of Data Points Using measuring test Instruments. Vendor has to arrange suitable cable certified (LAN certifier device) for CAT-6A for certification. Vendor must produce valid calibration certificate of the LAN tester before using it at site.

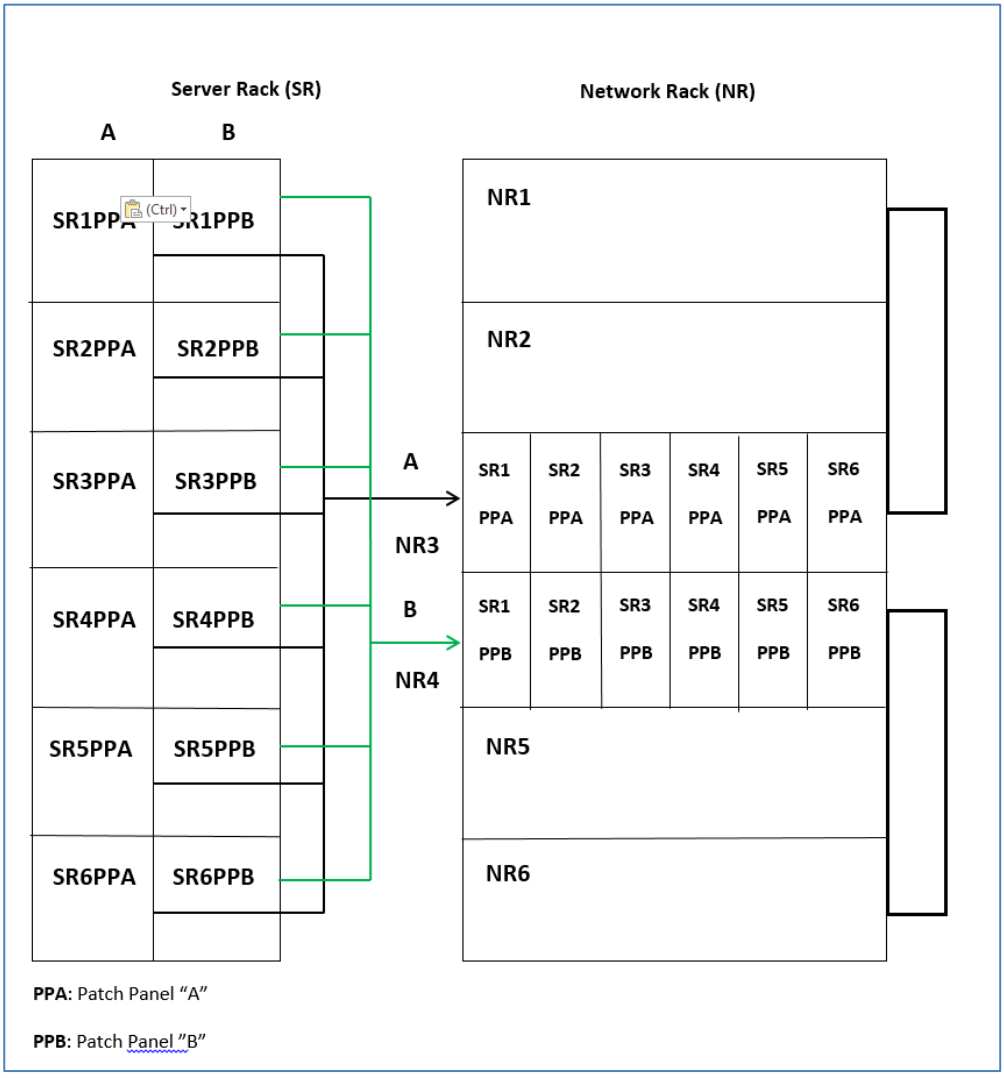


Figure: Shows the connectivity how racks needs to be provisioned with 10G structured cabling

Appendix 'J' – All in One PCs

a. **System Specifications -**

i. Pre-installed with Windows 11 Professional or latest version of windows

ii. Slots: Two DIMM, loaded with 16 GB memory configured

iii. Processor: Latest Generation Intel/AMD Processor with 14 cores, 2.5 GHz and 24 MB cache or higher processor.

iv. Hard Disk Drive: 1 TB SSD

v. Ports: USB Version 3.0 / 3.1, Ports: 4; USB Type C Ports: 1; VGA Ports: 1; HDMI Ports: 1; DP Port: 1; RJ-45 Ethernet Port – 1 No

vi. USB Multimedia keyboard and optical mouse

vii. POWER: 100-240V AC

viii. Required power adapter or Cable to be provided.

ix. The offered system will be all-in-one PC system and not a Personal Computer with independent Monitor, CPU, Speaker Webcam and Microphone. Vendors who offers solution on general purpose PC, will be rejected.

x. The hardware offered shall not have any in-built wifi interface and in-built Bluetooth interface. The system offered shall not have these features built on the chipset. If any vendor offer systems which has in-built wifi interface and in-built Bluetooth interface and is disabled through BIOS software, such systems shall not be accepted for evaluation. Vendor may note that, this is a security requirement and the compliance is must.

xi. System shall be delivered with OEM make 100mm VESA mount for mounting on work-console arms.

b. **Display Screen Specifications and features**

i. Display Size (INCHES): 23.8 or better

ii. Display Type: Non Touch

iii. Panel Technology: IPS

iv. Display Resolution (PIXELS): 1920x1080 or better

v. Availability of Webcam integrated with Display: NO

vi. Availability of Webcam integrated with Display: NO

vii. Availability of Speakers integrated with Display: Yes (two numbers)

c. **Certification**

   i. RoHS, BIS, BEE or equivalent international certification

   ii. TPM

   iii. Windows 11 certified

d. **Software to be included along with media with each PC -**

   i. Windows 11 Professional

   ii. Microsoft Office Professional latest version

   iii. Pre-loaded antivirus software with support for 5 years

e. **Bluetooth and WiFi: Should NOT BE integrated with the system. WEBCAM should not be present.**

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'K'– NMS Rugged Laptops

a. **Network Management System (Rugged Laptop)**

i. 14 inch fully rugged laptop

ii. Serial to USB Adapter – 2 Nos with each laptop

b. **Specification**

i. Pre-installed with Windows 11 Pro

ii. Intel core i-5 or AMD Processor

iii. 16 GB DDR4 RAM .

iv. 512 GB NVMe OPAL SSD

v. Ports: 2x USB 3.2, 1 HDMI out display port, 1 LAN

vi. Inbuilt microphone, camera and speaker

vii. Battery life upto 36 Hours (if required additional battery to be loaded in the configuration)

viii. 14 inch Full-HD Touch Active Matrix LCD, 1.200 d/m2

ix. DVD Multi Drive =1

x. Security – TPM 2.0

xi. Required power adapter and cable to be provided.

xii. IP66 Ingress protection

xiii. IP65 Dust Resistant

xiv. Drop Resistance = 180 cm

xv. Operating Temperature = -29 to + 63 degree celcius

c. **Software to be bundled along with each Laptop**

i. Windows 11 Professional

ii. Microsoft Office Professional latest version

iii. Antivirus software with 5 years subscription

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'L' – Automatic Transfer Switch (ATS)

Specification – ATS shall have following or better specification:-

a. **Input**

i. Input Connections =2 Nos.

ii. Nominal Input Voltage should be 220-240V

iii. Input Frequency = 47-63 Hz

iv. Input Connections should be IEC-320 C20

v. Maximum Line Current per phase =20A

vi. Maximum Input Current per phase =20A

b. **Output**

i. Output Connections=9

ii. Nominal Output Voltage = 220-240V

iii. Maximum Total Current Draw per Phase=16A

iv. Output Connections type IEC-320 C13=8

v. Output Connections type IEC-320 C19=1

vi. Overload Protection=No

c. **Physical:** 19 inch Rack mountable unit with rack mount kit. Rack Mounting Bracket or Mounting Rails should be included with the base product

d. **Front Panel**

i. Input Source Selection using push button with-out disturbing output should be possible

ii. Selected Source Should be visible on the front Panel

iii. Digital Display for current drawn per power Distribution

iv. Display should warn when current drawn is close to the maximum draw of the strip.

e. **Remote Management Capability –**

i. Offered product should be managed via Web ,SNMP , and Telnet

ii. Allows users to access , Configure , and manage units from remote locations

iii. Firmware should be upgradable via network

f. **High Availability:** Two AC Lines should power the Unit and if the primary AC power fails, the unit should automatically switch to the alternate power source within 20ms or without circuit breaker.

g. **Cooling:** Sufficient cooling shall be provisions

h. **Power Cord:** All Cables Should be RoHS Compliant. Power Cable shall be only from a proven product line from highly reputed manufacturers.

i. **Regulatory Compliance**

   i. Operating Environment: -5 to 45 degree C
   ii. Operating Relative Humidity: 5 to 95 %
   iii. Storage Temperature: -25 to 65 degree C
   iv. Storage Relative Humidity: 5 to 95 %

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'M' – Station Computers and AIO Thin Clients

Station Computer Server (STC) Server Specification

a. **Processor –**

i. Make & Architecture Intel CISC(X86-64),

ii. 8 Cores (16 threads) per processor or better,

iii. Processor Base frequency 2.6GHz,

iv. Processor Turbo Frequency 4.1 GHz,

v. Processor Description/ Number Intel Xeon Silver 4509Y or better or equivalent

b. **Chassis -** Form factor Rack, Size 1 RU

c. **Motherboard -**

i. Chipset compatible with CPU Intel C741 or better

ii. Expansion Slots Gen 3 (PCIe x16)- 1 or more

iii. Minimum number of Sockets populated with Processors on Server – 2 or more

d. **Memory –**

i. Type of RAM: DDR4 SDRAM with ECC or better

ii. Total Number of DIMM Slots: 32

iii. Minimum Number of DIMM Slots populated with DDR SDRAM: 2

iv. DDR SDRAM Size(GB): 128 or more

v. DDR SDRAM upgradable upto using spare DIMM Slots (GB): 960 or more

e. **SSD Storage –**

i. Type of Interface for SSD: SAS

ii. Type of SAS SSD: Mixed Use

iii. SAS SSD Hot Swappable: Yes

iv. Endurance for SAS SSD (DWPD - Drive Writes Per Day) (X): 1 or better

v. Total Number of Slots for SAS SSD: 8 or better

vi. Number of Slots shall populate with SAS SSD: 2 or more

vii. Minimum Capacity SAS SSD (GB) or more: 960 or better

viii. Total Capacity SAS SSD (GB) or more: 1920 or better

f. **RAID –**

i. RAID level: 1

ii. No of RAID Controller Ports: 8

iii. Speed of RAID Controller Ports (Gbps): 12

g. **Ports & Interfaces**

i. Network Card: 1G

ii. Number of Networking Interface Cards (LAN): 3

iii. Whether Network Interface Card Embedded: No

iv. Total Number of 1G Ethernet Ports required in Server: 10 X 1G

v. DVD-RW (Internal/External): Yes

vi. USB Ports (3.0) Minimum: 3

vii. Total number of Spare Bays for Future Upgradation (Hot Pluggable): 8 or more

h. **Certifications –**

i. Certifications/Compliance (OS) - Windows server 2022 standard edition or latest, Red Hat Enterprise Linux 9.2 or latest. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

ii. Compliance & Certifications – Following or equivalent international certification

- RoHS India [E-Waste (Management) Rules, 2016] certification
- Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard
- Security Compliance – TPM 2.0, UEFI Secure boot

i. **Operating System –** Redhat Enterprise Linux Server latest edition

j. **Management features**

i. IPMI 2.0 compatible management capability with dedicated management LAN

k. **Generic**

i. Redundant Power Supply - Yes

ii. Hot Swappable (Redundant Power Supply) - Yes

iii. Power Supply Efficiency - Platinum

iv. Redundant Fan - Yes

v. Hot Swappable (Redundant Fan) - Yes

vi. Server Main Supply - 230 +/- 10%Vac

l. **All in one thin client (AIO) for Display & Remote access with Specifications as below:**

i. Processor - 2.5 GHz or above.

ii. System memory- 8 GB DDR4 or above/better.

iii. Flash memory - 256 GB PCIe NVMe SSD or above.

iv. Display - 24 inch or above.

v. Display resolution - 1920 x 1080 FHD at 60 Hz, anti-glare or better and Color support 16.7 Million or better.

vi. Communications - 10/100/1000 Gigabit Ethernet (RJ-45).

vii. Ports & Connectors

viii. USB 2.0/3.0 = 2 minimum excluding the keyboard and mouse connections

ix. Gigabit Ethernet Port (RJ-45) = 1 or more. Display Port = 1 or more.

x. Power supply - 230 Volts AC, 50Hz, Built in power supply preferable.

xi. All-In-One (AIO) form factor is required with articulating stand.

xii. Sound bar with mic = 1 No.

xiii. System must not have any integrated Bluetooth and wireless adaptor.

xiv. Server and display should be from same OEM.

Software Configuration:

i. Protocols - RDP, PCoIP, Citrix, VMWare, view or other protocols required to support seamless remote access.

ii. Any device driver, protocol or license required to support the system **integration** to be provided by the vendor to complete the configuration.

iii. All in one thin client should be configured with embedded hardened OS which can support RDP/PCoIP to Servers with OS Windows Server 2022 or Latest version.

m. **Scope of supply**

Installation and Commissioning shall be included in the scope of supply.

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'N' – MCP Server and AIO Thin Client

M&C servers are deployed in BP1 & BP2 with 2 MCPs (Monitoring and Control Processors) and two GEIs (General Equipment Interface) in each station. These systems house the Monitoring and Control software that carries out schedule driven automatic configuration of the station as well as status monitoring of the station. Number of servers of GEI depends on the number of equipment deployed in the station. Current design of the software allows 50 equipment per GEI. The specifications for these servers are as below:

a. **Processor –**
   i. Make & Architecture Intel CISC(X86-64),
   ii. 24 Cores per processor,
   iii. Processor Base frequency 2.6GHz,
   iv. Processor Turbo Frequency 3.9 GHz,
   v. Processor Description/ Number: Intel® Xeon® Gold 6542Y 2.9G, 24C/48T, dual socket configuration or equivalent

b. **Chassis - Form factor Rack, Size 1 RU**

c. **Motherboard -**
   i. Chipset compatible with CPU Intel C741 or better
   ii. Expansion Slots Gen 3 (PCIe x16) - 1 or more
   iii. Minimum number of Sockets on Server - 2 or more
   iv. Minimum number of Sockets populated with Processors on Server – 2 or more

d. **Memory –**
   i. Type of RAM - DDR4 SDRAM with ECC
   ii. Total Number of DIMM Slots - 32
   iii. Minimum Number of DIMM Slots populated with DDR SDRAM - 2
   iv. DDR SDRAM Size(GB) - 128
   v. DDR SDRAM upgradable upto using spare DIMM Slots (GB) - 960

e. **SSD Storage –**
   i. Type of Interface for SSD SAS
   ii. Type of SAS SSD Mixed Use
   iii. SAS SSD Hot Swappable Yes
   iv. Endurance for SAS SSD (DWPD - Drive Writes Per Day) (X) 1
   v. Total Number of Slots for SAS SSD 8

vi. Number of Slots shall populate with SAS SSD 2

vii. Minimum Capacity SAS SSD (GB) or more 1.92TB

viii. Total Capacity SAS SSD (GB) or more 3840

f. **RAID –**

i. RAID level 1

ii. No of RAID Controller Ports 8

iii. Speed of RAID Controller Ports (Gbps) 12

g. **Ports & Interfaces**

i. Network Card 1G,10G

ii. Number of Networking Interface Cards (LAN) 3

iii. Whether Network Interface Card Embedded No

iv. Total Number of Ethernet Ports required in Server 6x 1G, 2X10G

v. DVD-RW (Internal/External) Yes

vi. USB Ports (3.0) Minimum 3

vii. Total number of Spare Bays for Future Upgradation (Hot Pluggable) 8

h. **Certifications –**

i. Certifications/Compliance (OS) - Windows server 2022 Standard Edition ,Red Hat Enterprise Linux 9.4 or latest. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

ii. Compliance & Certifications – Following or equivalent international certification

iii. RoHS India [E-Waste (Management) Rules, 2016] certification

iv. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

v. Security Compliance – TPM 2.0, UEFI Secure boot

i. **Operating System – Windows Server 2022 professional edition**

j. **Management features**

i. IPMI 2.0 compatible management capability with dedicated management LAN

k. **Generic**

i. Redundant Power Supply - Yes

ii. Hot Swappable (Redundant Power Supply) - Yes

iii. Power Supply Efficiency – Platinum

iv. Redundant Fan - Yes

v. Hot Swappable (Redundant Fan) - Yes

vi. Server Main Supply - 230 +/- 10%Vac

l. **All in one thin client (AIO) for Display & Remote access with Specifications as below:**

i. Processor 2.5 GHz or above.

ii. System memory 8 GB DDR4 or above.

iii. Flash memory 256 GB PCIe NVMe SSD or above.

iv. Display 24 inch or above.

v. Display resolution - 1920 x 1080 FHD at 60 Hz, anti-glare or better and Color support 16.7 Million or better.

vi. Communications - 10/100/1000 Gigabit Ethernet (RJ-45).

vii. Ports & Connectors

viii. USB 2.0/3.0 = 2 minimum excluding the keyboard and mouse connections

ix. Gigabit Ethernet Port (RJ-45) = 1 or more. Display Port = 1 or more.

x. Power supply - 230 Volts AC, 50Hz, Built in power supply preferable.

xi. All-In-One (AIO) form factor is required with articulating stand.

xii. Sound bar with mic = 1 No.

xiii. System must not have any integrated Bluetooth and wireless adaptor.

xiv. Server and display should be from same OEM.

- **Software Configuration**

i. Protocols-RDP,PCoIP, Citrix,VMWare View or other protocols required to support seamless remote access.

ii. Any device driver, protocol or license required to support the system **integration** to be provided by the vendor to complete the configuration.

iii. All in one thin client should be configured with embedded hardened OS which can support RDP/PCoIP to Servers with OS Windows Server 2022 or Latest version.

m. **Scope of supply**

i. Installation and Commissioning shall be included in the scope of supply - Yes

n. **Warranty**

i. As per Warranty Terms of the RFP

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'O' – 75 inch large scale display

1. 75 Inch size Large LCD Monitor

a. **Features**

i.	Screen Size	:	75" or Higher LED Back Lit Panel
ii.	Panel Technology	:	up to 50 (Single side) or higher
iii.	Native Resolution	:	3840 x 2160 (UHD)
iv.	Brightness	:	500cd/m2
v.	Contrast Ratio	:	1100 : 1 or more
vi.	Dynamic CR	:	500,000 : 1 or higher
vii.	Operating System	:	WebOS
viii.	Orientation	:	Portrait & Landscape
ix.	Viewing Angle(H x V)	:	178 x 178
x.	Response Time	:	8 ms or better
xi.	Operation Hours	:	24 Hrs support

b. **Connectivity**

i. **Input Ports**

Digital	:	HDMI(3), Display Port(1)
External Control	:	RJ45(1), IR(1, Internal)
USB	:	USB -1
Audio In	:	Audio In-1

ii. **AUDIO**

Audio Power	:	20W(10W x 2)

c. **Additional feature** **:** Inbuilt : Internal Memory 16 GB, Wi-Fi, Screen Sharing feature, Web Link, Media Player, Picture in Picture & Picture by Picture feature (4 Simultaneously), SNMP Support

d. **POWER**

i.	Power Supply	:	100-240V~, 50/60Hz

ii. Power Type : Built-In Power

e. **Certifications**

i. (Safety/EMC/ER) : UL, FCC,BIS, RoHS

ii. Wall mount : Required

2. <u>LCD Monitor Trolley Stand for 75 Inch</u>

a. **Features**

i. Shall have Large and sturdy base

ii. Shall have base with Lockable Caster wheel

iii. Shall have Height-Adjustable Camera Shelf

iv. Shall have Internal cable management for the cable routing (Preferable)

v. Shall have Vertical Height adjustable display mounting bracket (minimum 3 levels)

vi. Shall have Tilting Adjustment (Preferred Tool less for quick viewing adjustment)

b. **Technical Specifications**

i. Dimension, Height x Width x Length (mm) : 1840 x 680 x 1200 (+/- 20mm)

ii. Type : Heavy duty steel mobile LCD Display stand

iii. Screen Size : Shall support from 75 inch to 100 inch LCD Displays

iv. VESA Compatible : Shall compatible with VESA Mount dimensions of 200x200 to 1000x600

v. TV/Display Weight Capacity : Shall support Minimum 100kg

vi. Shelf Weight Capacity : Shall be Upto 20 KG

vii. Height Adjustment : Adjustable at three levels of 300/1380/1460mm (51.2"/54.3"/57.5") or equivalent or nearest slot level

viii. Tilt Range (Preferable) : +/- 10 Degrees

ix. Material : Steel structure with Black color powder coating matte finish

x. Certifications : CA 65 or equivalent

3. <u>HDMI male to HDMI Male cable (10mtrs and 20mtrs)</u>

a. **Features**

i.	Resolution resolution @ 60 Hz	:	Cable to shall support 4096x2160
ii.	Data rate	:	18 Gbps or better
iii.	Colour depth	:	8 bits per colour
iv.	Wire Gauge	:	Copper wire with 22 AWG
v.	Standards	:	HDMI 2.0 or higher
vi.	Connector type	:	Male HDMI to Male HDMI
vii.	Contacts	:	Gold plated
viii.	Jacket	:	PVC
ix.	Regulatory compliance	:	UL CL

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s).*

Appendix 'P' – Sys Log Server

Rack Server – Configuration -2

a. **Physical –** 19-inch rack mountable server of 1U rack mount size. Servers shall be offered with required rack mount hardware kit.

b. **Processor –** One Intel® Xeon® Silver 4510 (30M cache, 12 Cores, 2.4 GHz) or better or equivalent AMD processor on X86-64 architecture.

c. **Memory -** 128 GB ECC memory spread across all memory channels or better memory configuration.

d. **Internal Storage –** 2 Nos of 2 TB SATA Disk in RAID 1

e. **Drive Controller –** Internal RAID Card for RAID 1

f. **OS Certification:** RHEL & Windows certified hardware. All the required device drivers for RHEL shall be included in the offer. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

g. **Optical Drive –** Internal DVD RW drive to be offered

h. **Network Controller –** Total 4 nos of 1Gb Ethernet copper

i. **Ports –** Front :2 USB, Rear: 4 USB, VGA=1

j. **Power –**Hot Pluggable redundant power supply. Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

k. **Management -** Server shall include IPMI 2.0 compliant management module. Management function shall be offered on out of band over Ethernet.

l. **Cooling –** Server shall be configured with redundant cooling fans.

m. **Certifications – Following or equivalent international certification**

   i. RoHS India [E-Waste (Management) Rules, 2016] certification

   ii. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

   iii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

   iv. Security Compliance – TPM 2.0, UEFI Secure boot

n. **Operating System –** Redhat Enterprise Linux Server latest edition

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'Q' –SIEM Server

Rack Server – Configuration -3

a. **Physical –** 19-inch rack mountable server of 1U/2U rack mount size. Servers shall be offered with required rack mount hardware kit.

b. **Processor –** One Intel® Xeon® Gold 6548N Processor (60M cache, 32 Cores, 64 Threads, 2.80 GHz) or better or equivalent AMD processor on X86-64 architecture.

c. **Memory -** 512 GB ECC memory spread across all memory channels or better memory configuration.

d. **Internal Storage –** 10 Nos of 20 TB SAS 12G 7.2KRPM SAS Disk

e. **Drive Controller –** Internal RAID Card for RAID 1, 0, 10, 5 and 6 support with 8 GB Memory and 12G SAS interface

f. **OS Certification -** RHEL & Windows certified hardware. All the required device drivers for RHEL shall be included in the offer. The certification of the hardware shall be available in RHEL & Microsoft Web Site and listed in respective certified and compatible hardware list section with the model number of the offered hardware. Self-certification declaration shall not be considered for evaluation.

g. **Optical Drive –** Internal DVD RW drive to be offered

h. **Network Controller –** Total 4 nos of 1Gb Ethernet copper and four numbers of 10Gb Ethernet Copper port shall be configured for each server.

i. **Ports –** Front :2 USB, Rear: 4 USB, VGA=1

j. **Power –**Hot Pluggable redundant power supply. Power supply with 80% or better efficiency, Power Supply rating: 220 volt/50 Hz.

k. **Management -** Server shall include IPMI 2.0 compliant management module . Management function shall be offered on out of band over Ethernet.

l. **Cooling –** Server shall be configured with redundant cooling fans.

m. **Certifications –** Following or equivalent international certification

   i. RoHS India [E-Waste (Management) Rules, 2016] certification

   ii. Compliance to BIS norms for safety standard IS 13252:2010 or equivalent BIS standard

   iii. Energy Star 6.1 or equivalent – As per Bureau of Energy Efficiency, Govt of India Guideline for Computer

   iv. Security Compliance – TPM 2.0, UEFI Secure boot

n. **Operating System –** Redhat Enterprise Linux Server latest edition

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'R' – Colour Laser Printer

a. **Colour Laser Printer** **:** Duplex Colour Printing

b. **Printer Functions**

i.	Print speed (Color and Black):		27 ppm or more.
ii.	Duplex Print Speed (IPM) :		24 or better
iii.	Paper Size	:	A4.
iv.	Print Resolution	:	600 x 600 or better
v.	Print Technology	:	Laser
vi.	Control Panel: 2-line backlit LCD graphic display; 5 buttons (Cancel, Select, Reverse, Right/Left arrows); LED indicator lights (Attention, Ready)		
vii.	Processor speed	:	1200 MHz or better
viii.	Memory	:	512 MB or better
ix.	Display	:	2.7-inch(6.9cm) LCD with keypad or better
x.	Durability Ratings/ Duty cycle:		(No of Prints/month): 50000 or better

c. **Connectivity**

i.	Standard connectivity	:	USB 2.0 port, Ethernet 10/100 /1000 (1 Gigabit Ethernet) network port
ii.	Network capabilities	:	Yes (10/100/1000 Ethernet)

d. **Paper**

i. Input: 250 or higher100-sheet in main Tray, 50 or higher in Bypass Tray, 550 or higher in additional tray

ii. Yield of the cartridge/Ink Tank/Ink Pack supplied with Machine as per ISO/IEC - 19798/2007(E) for Cyan colour (Number of prints): 2100 or higher

iii. Yield of the cartridge/Ink Tank/Ink Pack supplied with Machine as per ISO/IEC -19798/2007(E) for Yellow colour (Number of prints): 2100 or higher

iv. Yield of the cartridge/Ink Tank/Ink Pack supplied with Machine as per ISO/IEC- 19798/2007(E) for Magenta colour (Number of prints) : 2100 or higher

v. Yield of the cartridge/Ink Tank/Ink Pack supplied with Machine as per ISO/IEC- 19752/2004(E) for Black colour (Number of prints) : 2400 or higher

vi. Duplex Print Options: Automatic (standard)

vii. Interfaces/Connectivity: 1 USB 2.0 Host ports; 1 Ethernet 10/100/1000 port

viii. Support Languages : PCL 6, postscript level 3 emulation, PDF

ix. Network Capability : 10/100/1000Base- Ethernet

x. Operating systems : Windows 10,11 and above; Windows Server 2016 and above 64-bit; Linux; Unix

xi. Power Supply : Built-in with power 230V +/- 10V AC 50-60 Hz

Note: *Refer sections in the RFP for establishing compliance towards Warranty, Installation & System support, Quality Requirements and instruction to bidders for the offered product(s)*.

Appendix 'S' – Black and White Laser Printer

a. **Black & white Laser Printer** : Duplex Printing

b. **Printer Functions**

i.	Cartridge Technology	:	Composite Cartridge
ii.	Print Speed	:	up to 50 (Single side) or higher
iii.	Print resolution	:	1200 x 1200 or better
iv.	Type of Printing	:	Mono (Black & White)
v.	Cartridge Technology	:	Composite Cartridge
vi.	Duplex print	:	Automatic
vii.	Duplex Print Speed (IPM)	:	34 (two sided) or better
viii.	Print technology	:	Laser
ix.	Standard print languages	:	PCL 6, postscript level 3 emulation, native PDF printing (v 1.7)
x.	Printer management	:	Through Keypad

c. **Connectivity**

iii.	Standard connectivity	:	USB 2.0 port, Ethernet 10/100 /1000 (1 Gigabit Ethernet) network port
iv.	Network capabilities	:	Yes (10/100/1000 Ethernet)

d. **Others**

i.	Memory	:	512 or better
ii.	Processor speed	:	1.2 GHz or better
iii.	Duty Cycle	:	Up to 150000 pages monthly or higher
iv.	Paper Input	:	550-sheet main input tray, 100-sheet in By pass Tray, 100-sheet Additional Tray
v.	Yield of the Cartridge pack supplied with machine as per ISO/IEC-19752/2004(E) for Black	:	5000 or higher
vi.	Paper / Media Size	:	A4, letter, legal, executive, envelopes
vii.	Operating systems support:		Windows 10,11 and above; Windows Server 2016 and above 64-bit; Linux; Unix
viii.	Display with Keypad:		2.7-inch (6.9 cm) LCD with keypad or better
ix.	Power Supply	:	Built-in with power 230V +/- 10V AC 50-60 Hz

Note: Refer relevant sections for establishing compliance towards Warranty, Installation & System support, Quality Requirements and Notes to the Vendor for the offered product(s).

Appendix 'T' – NMS Software

a. **Network Management Software -** The NMS Software should meet following requirement–

   i. **Monitoring Network Matrices -** Incoming and outgoing traffic, Total bandwidth usage, Packet loss and interface error rates, Number of TCP connections, Link status, auto discovery of connected devices

   ii. **Monitor Health -** Interface speed and status, Device availability and uptime, CPU and memory statistics, Power supply status, Device information, Temperature sensors, Fan states, Create dynamic problem thresholds for different resource types (e.g. trunk port or uplink port)

   iii. **Generate Alert -** React to unexpected network spikes, errors, packet loss, or ping loss; Analyze long-term bandwidth usage trends; Suppress alerts while performing device maintenance or upgrades; Dynamically detect anomalous network behaviour

b. **Server Monitoring**

   i. **Server performance -** High CPU or memory utilization, Network bandwidth usage, Packet loss rate, Interface error rate, Number of TCP connections is anomaly high for this day of the week, Aggregate throughput of core routers is low

   ii. **Server availability -** Free disk space is low, System status is in warning/critical state, Device temperature is too high / too low, Power supply is in critical state, Fan is in critical state, No SNMP data collection, Network connection is down

   iii. **Configuration changes -** New components added or removed, Network module is added, removed or replaced, Firmware has been upgraded, Device serial number has changed, Interface has changed to lower speed or half-duplex mode, out of the box template to monitor popular server and OS

c. **Service Monitoring –** Capability to monitor services in REHL and Windows OS.

d. **Application Monitoring** – Capability to monitor standard and integrate for custom application monitoring

e. **Log Monitoring** - Detect warning and error messages generated by an application, Receive alerts on security incidents by monitoring security logs, Visualize and graph the number of logged events

f. The platform shall have more than 300 internal templates built in for identification of popular products. Shall have Out of the box monitoring for leading software and hardware vendor.

g. The software shall support out of the box integration with leading ITSM systems

h. The monitoring software must be deployed on RHEL platform.

i. The monitoring software shall have agent for windows and linux hosts. The solution shall also have template for Proxmox Virtual Environment Monitoring.

j. **Support** – The monitoring software infrastructure should be upgraded to latest version once in a year or based on required upgrade based on latest features as required. All the implementation shall be migrated to new platform whenever such software upgrade is carried out. Vendor shall ensure all the configuration is migrated from existing platform to new platform during platform migration.

k. **License requirement** – The NMS platform shall need to monitor 35 Network Device (Including Switches and Routers), 160 hosts (including HCI infra, host and VM), 30 services and 30 applications. Suitable license shall be offered

Note: Refer relevant sections for establishing compliance towards Warranty, Installation & System support, Quality Requirements and Notes to the Vendor for the offered product(s).

Appendix 'U' –KVM and RKM

The quantity and specification of KVM and RKM are as mentioned below:

a. **Quantity**

i. No of IP console switches (KVM) = 1

ii. No of RKM Units = 2

iii. No. of USB interface adapter for KVM = 40

iv. No. of Serial Interface Adapter to Connect COM Port of Network/Servers for KVM=10

v. No. of Virtual Media Interface Adapter=01 No

vi. RKM, KVM and Adapters shall be of same OEM Make.

b. **Specifications for KVM Switch (Config 1):-**

i. No. of Target device ports per unit= 40 as a single unit (with out cascade)

ii. Supports up to 4 users as remote users over IP KVM Session and 1 local user

iii. Device shall have dual power supply

iv. Device shall have two NIC ports

v. Advanced FPGA graphics processor with HD resolutions up to 1920 x 1200

vi. High Video Resolutions – up to 1920 x 1200 @ 60 Hz with 24-bit color depth at the switch's local console and on remote displays

vii. Laptop USB Console (LUC) – a dedicated USB port directly connects to a laptop for easy console operation

viii. Supports PS/2, USB, Sun Legacy (13W3) and serial (RS-232) connectivity

ix. Local console provides USB keyboard and mouse support and same OEM make as the offered RKM

x. Supports multiplatform server environments: Windows, Mac, Sun, Linux and VT100 based serial devices

xi. Critical system event notification via SMTP email; SNMP trap and Syslog support

xii. IPv6 capable

xiii. Supports TLS 1.2 encryption and RSA 2048-bit certificates to secure browser logins

xiv. Virtual media enables applications, OS patching, software installations and diagnostic testing

xv. Console port - 2 x USB Female (Black) 1 x DVI-I Female (White)

xvi. Form-Factor: 1U Height with 19” Rack Mountable Option

xvii. Remote virtual media - Easily load and update software and firmware from anywhere on the LAN or WAN when used with Virtual Media Interface Adapters.

xviii. Internal dual power supply with rated Voltage 100 to 240V AC at 50 to 60 Hz should be offered

c. **Specifications for KVM Switch (Config 2):-**

i. No. of Target device ports per unit= 8 as a single unit (with out cascade)

ii. Supports up to 4 users as remote users over IP KVM Session and 1 local user

iii. Device shall have dual power supply

iv. Device shall have two NIC ports

v. Advanced FPGA graphics processor with HD resolutions up to 1920 x 1200

vi. High Video Resolutions – up to 1920 x 1200 @ 60 Hz with 24-bit color depth at the switch’s local console and on remote displays

vii. Laptop USB Console (LUC) – a dedicated USB port directly connects to a laptop for easy console operation

viii. Supports PS/2, USB, Sun Legacy (13W3) and serial (RS-232) connectivity

ix. Local console provides USB keyboard and mouse support and same OEM make as the offered RKM

x. Supports multiplatform server environments: Windows, Mac, Sun, Linux and VT100 based serial devices

xi. Critical system event notification via SMTP email; SNMP trap and Syslog support

xii. IPv6 capable

xiii. Supports TLS 1.2 encryption and RSA 2048-bit certificates to secure browser logins

xiv. Virtual media enables applications, OS patching, software installations and diagnostic testing

xv. Console port - 2 x USB Female (Black) 1 x DVI-I Female (White)

xvi. Form-Factor: 1U Height with 19” Rack Mountable Option

xvii. Remote virtual media - Easily load and update software and firmware from anywhere on the LAN or WAN when used with Virtual Media Interface Adapters.

xviii. Internal dual power supply with rated Voltage 100 to 240V AC at 50 to 60 Hz

should be offered

d. **Specification for RKM Units**

i. **Specification**

1) 1U rack-mountable with integrated monitor, keyboard & mouse functionality
2) Rail Type: Dual Rail
3) Shall be of same make of OEM for KVM units
4) Input Video Resolution up to 1920 x 1200 @ 60Hz
5) Mode (Output) 1920 x 1080 @ 60Hz
6) Compatible with Windows and Linux
7) **Keyboard/Mouse Emulation:** USB connectors
8) No of VGA IN Ports=1
9) No of HDMI = 1 No
10) Monitor shall be mounted inside the foldable lid that covers the keyboard
11) Keyboard shall have minimum 88 Keys layout including trackball mechanism for smooth navigation in the base.

ii. **Display Type:**

1) Flat-panel, LCD
2) 18.5" TFT-LCD or better
3) Maximum Input Graphics Resolution 1920 x 1080 @ 60Hz
4) Response time <25ms
5) Contrast ratio – 1000:1
6) Viewing Angle : 178
7) Color : 16.77M colors
8) Luminance >= 300(cd/m^2)
9) On Screen Display (OSD) Controls should support English language and should provide option for Brightness, contrast, positioning, color temperature, individual color control, input selection, factory reset

iii. **Certification and Compliance**

1) ROHS
2) Energy Star Compliant

e. **USB Interface adapter for KVM:** USB interface Adapter is required to connect End-Devices, specifically Servers with VGA-Out and not having PS2 Keyboard and mouse ports to the KVM console Switch.

f. **Serial Interface adapter for KVM:** To connect Serial port devices over 9-pin serial console port to KVM switch.

Note: Refer relevant sections for establishing compliance towards Warranty, Installation & System support, Quality Requirements and Notes to the Vendor for the offered product(s).

Appendix 'V' – SIEM Software with 3500 EPS

SIEM (Security Information and Event Management) Solution: solution for 3500 EPS or 100GB per day data license capacity.

a. **Requirement**

i. The solution shall be delivered as a VM ready solution deployable over KVM or equivalent virtualization platform. If the solution requires proprietary VM infrastructure, vendor shall include the required licenses for VM platform.

ii. The solution shall be deployed as a multimode server cluster may be delivered as a native or offered as a third party solution. Any license requirement shall be offered by the Vendor.

iii. The solution shall be deployed with purpose-built operating system. In case the solutions use generic operating system platform it must be limited to only Linux or Debian.

iv. The offered platform shall have following compliances –
1) SOC -3 Compliant product
2) ISO 27001, ISO 27017 and ISO 27018 compliant
3) Support Section 508 compliance

b. **General**

i. The solution shall offer enterprise-grade security and developer-friendly APIs to machine learning and graph analytics with features to ingest, analyse, search, and visualize all types of data at scale.

ii. The solution shall be highly scalable cluster as a collection of one or more nodes (servers) that together holds all of data and provides federated indexing and search capabilities across all nodes. The cluster set also provides availability by providing features like failover. Internal rebalancing occurs every time a node exits or join the cluster to provide distribution of data.

iii. The offered solution shall be horizontally scalable as demand increases. The platform shall support cross cluster replication which is rack aware and site aware.

iv. The solution shall have visibility into platform environment and can control how long the data set to be retained with the environment.

v. The solution shall be manageable via variety of management tools including UIs, APIs etc.

vi. The solution shall allow the administrator to define the Index life cycle management and define Hot, Warm, Cold/Frozen and Delete operation on the Indexes. The solution will allow to create data Tiers (Hot, Warm, Cold) accordingly.

vii. The solution shall have native snapshot capability to protect its data from accidental modification. The snapshots can be stored in a repository on a shared file system. The solution shall have capability to directly query the snapshots. The snapshot life cycle management capability shall also define the lifecycle of the snapshot provide native with the platform.

viii. The solution shall support snapshot based peer recoveries.

ix. The solution shall provide features like data rollup which will create only summary of actual data and discard detailed data.

x. The solution shall support data ingest capability via Data Stream.

xi. The solution shall provide CLI tools for managing the interface along with Web UI for the same.

xii. The solution shall provide suitable Upgrade UI which will assist to identify the deprecated settings in your cluster and indices, guiding you through the process of resolving issues — including re-indexing.

xiii. The solution shall allow to create user and roles via API and UI.

xiv. The solution shall support representing data in Transforms and directly digestible for ML.

xv. The platform shall provide full stack alerting mechanism (for email, IBM Resilient, Jira, Microsoft Teams, PagerDuty, ServiceNow, xMatters, and Slack. Integrate with any other third-party system via a weblook output)for events and query based results

xvi. The solution shall provide control of the alerts by viewing and managing all of them from a single UI. It shall provide features for alert suppression and noise reduction in UI mode. It shall support alerts based on triggers like incidents satisfying internal rules.

xvii. The solution shall have access rights mechanism to provide granular access to users on control their rights on data and operation. The solution shall support Role-based access control (RBAC) and Attribute-based access control (ABAC). Internal keystore (password protected) mechanism shall provide additional layer of security.

xviii. The solution shall use encrypted communication channel between nodes using SSL/TLS

xix. The solution shall provide easy sharing mechanism of dash board with anonymous users without compromising security of the infrastructure.

xx. The solution shall have field-level security which restricts the fields that users have read access to. It shall restrict which fields can be accessed from document-based read APIs.

xxi. The solution shall support security features like audit logging, IP filtering, Security realms , Single Sign on, third party security integration

xxii. The offered solution shall support Section 508 compliance standards and shall meet to meet Section 508 compliance standards.

xxiii. The offered solution shall support working on data anywhere with RESTful APIs, language clients, robust DSL

xxiv. Data ingestion: Solution shall collect security events and logs from various sources, including network devices, endpoints and third-party security tools. It shall support following device and application context

1) Network Devices including Switches, Routers, Wireless LAN
2) Security devices — Firewalls, Network IPS, Web/Email Gateways, Malware Protection, Vulnerability Scanners
3) Servers including Windows, Linux, MAC
4) Infrastructure Services including DNS, DHCP, DFS, AAA, Domain Controllers, VoIP
5) User-facing Applications including Web Servers, App Servers, Mail, Databases
6) Cloud Apps including AWS, Box.com, Okta, Salesforce.com
7) Virtualization infrastructure including VMware ESX, Microsoft Hyper-V Scalable.

xxv. Advanced analytics: The solution shall provide machine learning and advanced analytics techniques to identify anomalies, patterns and potential threats in the collected data. The platform shall allow searching features as follows -

1) Search events in real time— without the need for indexing
2) Keyword and event-based searches
3) Search historical events — SQL-like queries with Boolean filter conditions, group by relevant aggregations, time-of-day filters, regular expression matches, calculated expressions — GUI and API
4) Use discovered CMDB objects, user/ identity and location data in searches and rules
5) Schedule reports and deliver results via email to key stakeholders
6) Search events across the entire organization, or down to a physical or logical reporting domain
7) Dynamic watch lists for keeping track of critical violators — with the ability to use watch lists in any reporting rule
8) Scale analytics feeds by adding Worker nodes without downtime

xxvi. The solution shall support scalable and flexible log collection. The features shall support -

1) Collect, Parse, Normalize, Index, and Store security logs at very high speeds
2) Out-of-the-box support for a wide variety of security systems and vendor APIs — both on premises and cloud
3) Windows Agents provide highly scalable and rich event collection including file integrity monitoring, installed software changes, and registry change monitoring

(Process, file, network, DNS, driver and DLL loads, registry, malware security detections)

4) Linux Agents provide file integrity monitoring, syslog monitoring, and custom log file monitoring (Process, file, network)
5) Modify parsers from within the GUI and redeploy on a running system without downtime and event loss
6) Create new parsers (XML templates) via integrated parser development environment and share among users via export/import function
7) Securely and reliably collect events for users and devices located anywhere

xxvii. The solution shall support active agents on hosts which shall work as Detection engine, Timeline, Cases and administration of hosts that runs active agents

1) Active Agent: Automatically searches for unusual network and host activities using:
    - Detection rules: Regularly scan data from the hosts for abnormal events. When a suspicious event is found, the engine generates an alert.
    - Exceptions: Decrease noise and false positives by associating exceptions with rules, preventing alerts when exception conditions are met. Value lists include source event values that can serve as part of the exception conditions.
    - Machine learning jobs: Automatically detect anomalies in network and host events. Anomaly scores are given for each host and can be combined with detection rules.
    - Timeline: A workspace for examining events and alerts. Timelines employ queries and filters to probe into events related to specific incidents.
    - Cases: An in-app system for opening, sharing and tracking security issues within the Security application. Cases can be integrated with a ticketing system.
    - Administration: Monitor and manage hosts that run active agent

xxviii. Incident response and case management: The platform shall include case management features that help security teams to organize and manage security incidents. This streamlines the incident response process, enabling teams to collaborate more effectively and resolve security issues faster. The features include -

1) Automation and Incident Management
2) Policy-based incident notification framework
3) Ability to trigger a remediation script when a specified incident occurs
4) API-based integration to external ticketing systems
5) Built-in Case Management system
6) Incident reports can be structured to provide the highest priority to critical business services and applications
7) Incident Explorer — dynamically linking incidents to hosts, IPs and user to understand all related incidents quickly

xxix. Real-time monitoring: The solution shall allow security teams to monitor security events, manage logs and receive real-time alerts, providing a comprehensive and up-to-date view of an organization's security posture.

xxx. The solution should have ability to leverage MITRE ATT&CK Framework integration within events\incidents (ID, Tactics, Technique). The solution repository should have Activity data as well as Detection data (which should be mapped to MITRE TTPs framework)

xxxi. Customizable dashboards: The solution shall provide pre-built dashboards and visualization tools which enabling security teams to create custom views and visualizations of security data.

xxxii. Alerting and notifications: The offered solution shall provide a flexible alerting system that allows security teams to create custom rules and receive notifications on potential threats. This helps ensure that teams are promptly alerted to critical security incidents.

xxxiii. Threat hunting: The offered solution shall enable proactive threat hunting by providing powerful search and analytics capabilities, allowing security teams to investigate potential threats and uncover hidden patterns.

xxxiv. Support – Vendor must offer OEM support for single node implementation for the support duration.

Appendix 'W' –Network Behavior Analytics (NBA/NBAD)

a. The solution should be an appliance based solution – delivered as an OEM certified appliance as an integrated package.

b. The solution shall have collector or sensor and analytics as two different component for flexible deployment in the existing network, with-out changing any configuration in the network. It shall be possible to control the analytics node from a master node/ central node for monitoring and configuration.

c. The collector shall have capability to keep raw data for 3 Days and normalized data for 100 days locally. Beyond 100 days the normalized data/metadata to be pushed to central syslog.

d. The license capacity of the traffic must be calculated based on average throughput of 7 days and not by peak throughput of the interface. The license capacity must ensure total average throughput of 5 Gbps full-duplex when aggregated across all the network segments and must not pose limitation based on network segment.

e. The networks for which the details are shared above shall have overlapping IP address range. The solution must support working with overlapping IP addresses, keeping context of the network preserved.

f. The solution should be on premise and should not require internet access for day to day functionality. Any required update should be supported offline.

g. The solution must be an out of band analytics engine from the primary data path.

h. The solution shall be designed along with its associated component as a monitor only capability to ensure no data is ingested in critical network. Suitable datasheet and hardware details to be shared with the offer.

i. Throughput – The product must be licensed for total 7 Gbps average throughput

j. The solution must be designed to collect data from three networks minimum per site as follows –

    i. Network X – Directly connected on the NBA platform with 3 Gbps Full Duplex span/mirror traffic

    ii. Network Y – Connected via isolation mechanism (Isolation at Layer -1) to ensure only one way traffic is ingested to the NBA with 1 full duplex Gbps Span traffic

    iii. Network Z – Connected via isolation mechanism (Isolation at Layer -1) to ensure only one way traffic is ingested to the NBA with 1 Gbps full duplex Span traffic

k. The vendor shall provide detailed design to ensure the isolation mechanism is established in the media and not on higher layer (Layer 3 or higher). If the isolation is achieved in higher layer (Layer 3 or more) then the offer will be technically rejected.

l. The solution must be able to maintain the context of the network where the data is collected.

m. The solution must be able to analyze and forward extracted metadata to syslog. This syslog data must be ingested to the SIEM for further analysis

n. The sizing of the solution must match traffic aggregation bandwidth criteria as mentioned above.

o. The solution must capture live span/port mirror traffic of the network of interest and shall be able to capture the data.

p. Proposed NBA/NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc

q. Responsibility of configuring the switches for successful deployment of proposed NBA/NBAD systems lies with the supplier

r. The solution should maintain an updated 90-day profile (minimum) of all devices including a summary of protocol history to aid in the discovery of low-and-slow attacks.

s. The solution should provide contextual network-wide visibility via completely agentless approach.

t. The NBA/NBAD tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NBA/NBAD integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.

u. The solution should provide an independent and comprehensive analysis of the attack surface by uniquely identifying and profiling endpoints (Windows, MacOS, Proxy machines, Phones, Printers, IoT, etc.) based on behavioral fingerprints irrespective of IP address changes.

v. The solution must support minimum 20 ML models for enhanced detection and should not rely on only Rules/IOCs for threat identification.

w. The solution using AI-driven security must be able to autonomously build a case management collecting artifacts on its own and attaching them to the case management without any human intervention.

x. The solution should support and provide examples for minimum two of the , of the following data science methods. Details with examples on how each of these data science methods are used should be provided and demonstrated as part of the proof of concept evaluation if required (corresponding ML model to be provided).

    i. Supervised machine learning

    ii. Unsupervised machine learning

    iii. Deep neural networks

    iv. Belief propagation

    v. Multi-dimensional clustering

vi. Decision tree classification

vii. Outlier detection

y. The solution should be able to provide real-time monitoring and visibility into all network traffic, using machine learning, context-aware analysis, and on-premise threat detection and analytics.

z. The solution shall use behavioral technology and machine learning and advanced entity modeling to reduce false positives. Solution should detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.

aa. The solution must fully expose the definitions for all out of the box vendor provided threat detection techniques (models/Rules/ML/etc) and allow for their easy modification or adaptation.

bb. The NBA/NBAD solution should also offer the flexibility and capability to drill down into the end user, MAC, flows, interface utilization and a wide array of other host statistics needed for rapid incident resolution. Should utilize anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration.

cc. The solution should be able to natively identify the fingerprints from network traffic including but not limited to domains, ciphersuites exchanged in TLS handshake, HTTP body hash etc. All the fingerprints which uniquely identify the devices should be clearly grouped together and provide count of the times the fingerprints were seen on the network.

dd. The solution should detect threats in encrypted traffic without the need to decrypt or only comparing JA3 hash values. For example, the solution should check the commonality and frequency of TLS ciphers and destinations, without requiring support from existing network switches, endpoint agents, network proxies or threat intelligence feeds.

ee. By collecting, analyzing and storing available log information from various sources, NBA /NBAD System should provide a full audit trail of all network transactions for detecting anomalous traffic and performing more effective forensic investigations.

ff. The solution should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.

gg. The solution should provide use cases to identify usage of insecure, legacy and deprecated encryption algorithms being used by servers on the network.

hh. The solution must detect unusual, unauthorized behavior within the network. This includes but is not restricted to unusual RDP, port scanning, unauthorized new devices plugged in, unauthorized use of access credentials to internal resources.

ii. The solution should have DNS Threat Analytics Capability to detect the threat present in DNS traffic, DNS spoofing and DNS tunneling attack.

jj. The solution should highlight weak ciphers being used in the network by hosts or applications. The solution should search and monitor cipher suites and report on which ones are used on the network.

kk. The solution should be capable of rejecting particular network data from analysis using input filters. For example, exclude Video surveillance data from being processed by the NBA/NBAD solution

ll. The solution must support VPN tunnel detection for private and anonymous VPN tunnels and just not the VPN used by the Organization. Privacy VPN - Personal VPN solutions which enable the user to avoid network monitoring solutions

mm. The solution must support port-agnostic protocol detection. The Solution must be capable of conducting protocol analysis to detect applications using unexpected ports, anomalous transfer of data via certain protocols indicative of tunneling activity, backdoors, and the use of forbidden application protocols

nn. The solution must provide support for various OT protocols such as modbus, profinet, cip, bacnet_app,opcua, iccp, honeywell_phd,s7comm, bacnet_net,pccc, iec104, dnp3, goose, vnetip, bacnet_vlc, deltav, mqtt, etc. Minimum 10 OT protocol must be listed in datasheet.

oo. The solution must distinguish between similar devices based on unique fingerprints (including unmanaged & IOT) and provide commonality & frequency analysis for each such fingerprint to minimize the false positive rate. Must automatically group similar devices together based on a combination of fingerprints, provide an explanation of the similarity, and identify packet captures corresponding to that fingerprint for forensic and outlier analysis.

pp. The solution should identify the presence of botnets in the network. and detect long-lived connections that may be associated with data-exfiltration.

qq. The solution must provide APIs to integrate with existing security solutions like Security Information and Event Management (SIEM), Next-generation Firewalls, Router, Switches, NAC, SOAR, Proxy, WAF, Mail gateway etc. Necessary applicable licenses for integration with other security devices must be supplied from day one

rr. The solution should support all the following features without exception, under the incident management workflow component with built-in automation that automatically:

    i. Visually maps out the devices and external destinations involved in the incident

    ii. Visually maps the relationships between the devices involved using machine learning and not solely based on simply correlating all connections to a known malicious IP or domain.

    iii. Use natural language processing and topic modelling to add context to the incident

    iv. Provide a complete audit of the automated investigation.

    v. Mark legitimate activities of the devices involved during the time of the incident

    vi. Suppress activities that are not relevant to the attack automatically.

    vii. Automatically generates an incident of the attack when new traffic is added.

    viii. Provide a PDF report of the incident.

ss. The solution should have capability to assign risk and credibility rating to alerts and hosts and present critical high-fidelity alerts prioritized based on threat severity with contextual

information on the dashboard.

tt. For each and every device that uses multiple IP addresses due to DHCP over a period of time, the system must display all the previous IP addresses linked to this device on the GUI along with the most recent IP address assigned to the device.

uu. The solution must show on the GUI when the device was first seen for all the devices being monitored by the system along with the last active timestamp.

vv. The solution should have integration with the MITRE ATT&CK matrix and also should mandatorily show the suggested mitigation recommendation for each of the TTPs in ATT&CK matrix.

ww. The system should have a mechanism to consume external lists of known bad IP's and generate alerts on the same if connection is seen.

xx. The solution should also have the capability of threat intelligence management where the custom threat intel IOCs can be added by the user

yy. Storage Calculation – The total storage for the solution must be computed as follows -

i. Average Packet Size (Raw and Metadata) – 576 Bytes

ii. Total Numbers Packet in the 5 Gbps full duplex Link – 1785714 (Considering 80% capacity in full duplex mode)

iii. Number of Days of Storage Required for raw Data – 3 Days

iv. Number of Days of Storage Required for Meta Data – 100 Days

v. Link Utilization considered – 100% full duplex

vi. Raw data Storage –240 TB, If OEM support compression proportionately reduction in storage shall be considered. However, suitable datasheet or evidence to be provided.

vii. Meta data Storage – 75 TB, If OEM support compression proportionately reduction in storage shall be considered. However, suitable datasheet or evidence to be provided.

Appendix 'X' – One time Implementation and Documentation

System Integration, Implementation, Service Migration and Security Audit

a. **General Instruction -** Vendor shall carefully go through the scope of system installation, service migration and security audit requirements and accordingly propose the solution:

   i. Vendor to note that, as user site is an operational setup and vendor needs to deploy and migrate operation to new hardware, Vendor must prepare step by step plan of system deployment/implementation and service migration activity.

   ii. Vendor must make a rack layout plan and work out how the old hardware will be removed and new hardware will be integrated in the rack along with service migration. The integration and migration activity involves existing 12 nos. of 42U standard racks. Vendor must note that all the deliverables may not be accommodated in the server rack without removing the old hardware from the operation. Hence a sequence of planned migration must be worked out by the vendor. The same needs to be presented to NSIL/User team.

   iii. Vendor must note that, the planning activities on system implementation and service migration activity may start prior to the actual hardware delivery to reduce the installation and implementation timeline.

   iv. This may be noted that, Vendor team has to study the existing configuration and make detailed migration plan document and present it to NSIL/User Team for plan review and approval. It is responsibility of vendor to migrate operations without extra downtime

   v. Vendor shall ensure for each specific activity, expertise in skills are available on site for system implementation and service migration activity

   vi. It may be noted that, for any service migration task, maximum two hours downtime will be acceptable and will be provided as a continuous span of two hours during any time of the day in concurrence with NSIL/User. The migration process must have plan for each network component, time split-up with respect to activity wise, considering fall back scenario for each service migration.

   vii. It may be noted that vendor will be provided access to the existing setup (in read only mode) to understand the configuration of each element and workout the service migration plan. It is responsibility of the vendor to understand various dependencies in the configuration and perform successful migration of service without disrupting the existing operation. Vendor should build required test setup to demonstrate the User/NSIL team on success of the plan before implementing at actual wherever required. Each service migration will be examined in operation for final acceptance by

User/NSIL team.

viii. Vendor may note that the section below broadly describe the scope of work. However the delivery will not be limited only to mentioned points. NSIL/User may ask to implement any of the features which are part of product specification and required for NSIL/User implementation. Ex. WORM feature for Storage, Virus Scanning Feature for Storage, and File system audit configuration for storage. Considering this fact, vendor must review the product capabilities asked and shall support delivery of and to demonstrate of suitable features during product implementation.

b. **Service Migration:** Vendor shall carry out following service migration activity:

i. **LDAP/NIS:** Understand the existing implementation of LDAP/NIS and hosting new LDAP infrastructure. Migration of user database and attributes to newly hosted LDAP server and successful demonstration of operation of User control center with new LDAP. Vendor shall also implementation the recommended security hardening based on the OS platform and application software. The migration will be functionally accepted when User operation is successful for twenty four hours even after shutting down of the existing (old) LDAP/NIS severs.

ii. **Storage and Backup:** Understand the existing implementation of storage and backup policy and accordingly create required aggregates, volumes , snapshots and file system on the new storage. Migration of data to the new storage with-out changing the attribute of data types. Vendor shall use suitable data synchronization tools/software's to ensure the file attributes are not changed during synchronization process. The backup configuration shall ensure current backup features are available. Vendor shall also implementation the recommended security hardening as per OEM recommended practices for Storage and Backup environment. The migration will be functionally accepted when User operation is successful for twenty four hours even after shutting down of the existing (old) Storage Servers.

iii. **Operation migration of FTP/SFTP and Rysnc Configuration:** Vendor shall study the configuration of FTP/SFTP and Rsync host / service configuration and replicate the same configurations on new hardware on latest version of operating system along with security hardening (SELinux, Host Firewall etc). The FTP log shall be configured in vivid mode to record essential details. The migration will be considered successful once the operation is successful for twenty four hours even after shutting down of the existing (old) systems.

iv. **Migration of Real-time Distributors:** Configuration of Realtime data Distribution system will be provided on new hardware by providing identical network configuration of the system along with all the required hardening. NSIL/ISRO/User team shall migrate the application software to new data

distribution server. There will be two such servers in the configuration and migration shall be done one by one on different working days. NSIL/ISRO/User application team will verify the success of the migration.

v. **Syslog Service Migration:** Configuration of SysLog server will be carried out based on existing configuration and shall be integrated with all the elements with proper log organization and rotation. The Syslog host will be provided with 1TB NFS area which will be only mounted for Syslog node in read-write mode and will be available to other nodes (if required) in read-only mode. This configuration shall be restricted from Central NAS storage. The migration will be considered successful after verification of all device log getting recoded in the new hardware for two days after shutting down the existing (old) system. The required configuration to push Syslog to the Syslog server needs to be configured in entire pool of systems (Router, Switch, server, Workstation, Tape Library, SAN Switch, VMs etc) as part of implementation.

vi. **Ansible Service –** Vendor needs to migrate the Ansible implementation to the new infrastructure on latest version of the software. Vendor also need to add new playbook as and when required.

vii. **NGFW Migration -** Configuration of UTM Device shall be carried out by deployment of UTM manager with suitable internet connection (As per provided connection by User) and integrating the UTM with Manger for configuration management patch update. The UTM Manager and Analyzer Device shall be updated to latest stable version before configuration of UTM Device. The vendor shall review the configuration of existing UTM and build the policy accordingly in the new UTM keeping the resource, service and groups name identical. Vendor shall ensure the services are built with suitable controls of IPS, IDS and Antivirus feature and shall successfully demonstrate detection of malformed traffic if attempted to transfer via the interface. The physical interfaces shall be labelled as per requirement. Once all the policies are built, it will be reviewed by User/NSIL team and shall be given authorization for migration of the services. The UTM overall environment will be monitored for two working days for complete review of Manager, Analyser and traffic flow behavior and declare as complete. Vendor may also note that, the new UTM may need creation of additional partition for integration of ground station M&C network to the same device. Required policies and guidelines shall be provided by User team during implementation. The vendor shall also integrate the Enterprise End Point Management System (EMS) and end point protection software with the security fabric and enable suitable policies for identified endpoints.

viii. **Router configuration–** The routers are deployed at User Control Center and other interfacing locations. Vendor needs to study the configuration of the existing (old) routers and replace the configuration with new router hardware. The vendor shall ensure the router firmware is updated to latest version of

the image/firmware before deployment. Where ever required, IPSEC tunnels will be established with QoS (Quality of Service) and required VRFs will be created for service isolation as per NSIL/ISTRAC/User requirement. Vendor shall also ensure the recommended security configuration for the router will be implemented as per OEM best practices and guideline. The User team shall verify the configuration and observe successful operation for two working days before acceptance of the configuration.

ix. **Switch configuration -** Vendor shall ensure the all the existing switches will be replaced by newly delivered switches and configuration will be ported to the new hardware. All the switches shall be placed on latest version of stable firmware as per OEM recommendation before deployment. The switches shall be security hardened as per OEM recommendation. Vendor shall also enable 802.1x (port security) as per requirement of User team. The User team shall verify the configuration and observe successful operation for two working days before acceptance of the configuration.

x. **RKM and KVM -** The vendor shall integrate the RKM and KVM infrastructure with the newly delivered elements and connect all the equipment to the management port as per requirement. The management network will be a completely isolated network from data network. The management interface shall be used for update of firmware and device drivers for various hardware elements wherever feasibility exists. The User team shall verify the integration process and observe successful operation for two working days before acceptance of the configuration

xi. **Management Interface -** Vendor shall study the management configuration interface and bring all the devices with management port to a single management network fabric. Vendor shall ensure that the management LAN shall be deployed with a LDAP Server / VM and users shall have dedicated named account for access of Management Interface. Every device shall have read-only and super admin account and shall be mapped to user roles. The management LAN shall also have syslog configuration for collecting event logs from each hardware.

xii. **Workstation Configuration -**Vendor shall install the latest RHEL packages as per provided package list and shall ensure the Nvidia drivers and associated configurations are configured.

xiii. **Host/VM Host Environment Configuration:** Vendor needs to install RHEL OS in respective hosts (server, workstation, VM instance for total around 150 nodes/instances) and shall configure the following

1) Operating system installation and registration/ activation wherever required.
2) Device driver installation
3) Dual-display configuration (only for few workstations)
4) Network and timing configuration

5) NIS/LDAP Client, Network and Channel Bonding and NFS configuration
6) SELinux, Host Firewall and Peripheral Device control policy implementation
7) FAPolicy configuration

c. **System Implementation:** The following new interfaces will be implemented by the Vendor as per detailed requirement. The detailed requirements will be provided by User/NSIL team and accordingly vendor has to prepare plan of implementation along with details of resources, network plan, interconnect diagram etc for approval by User/NSIL team. Vendor shall ensure sufficient care taken to avoid any disruption in operation during the process of Implementation.

i. **Data Diode:** Vendor shall configure the data diode (provided by NSIL) for movement of files from external network to internal network via Data Diode1 and Internal network to External Network via Data Diode2. While a file is copied from External network to internal network, the file will be scanned via antivirus software before further movement to the internal network. The interface system in the internal network will be made as a staging system where the Anti-Virus engine will scan the file before further delivery to the internal path. The completion of this interface shall be verified by moving files in and out of the User LAN via data diode interface. Vendor may note that the data diode hardware will be provided by NSIL along with configuration guide. Vendor has to provide the integration and antivirus / host protection software configuration along with file delivery path.

ii. **End Point Protection and Control:** Vendor will establish the Antivirus Central server infrastructure which will be deployed in User internal network and shall provide virus protection for all the FTP server, Data Diode interface server and any other node which is required for protection. The Vendor shall make arrangement via data diode interface to bring regular database updates for the anti-virus engine or via integration with NGFW Fabric. The success of the implementation shall be verified by successful detection of the test malware placed by User team during acceptance and through verification of the automatic update process.

iii. **Monitoring Dashboard:** Vendor shall configure monitoring dashboard using the management and monitoring software as follows –

1) Network WAN View –This view shall show the live status of connectivity with User and other entities with the description of the links. With this dashboard view, operations team shall make out any connectivity issues (on WAN) and shall represent live status of the link in healthy, degraded or down mode.
2) Network LAN View – This view shall show the critical LAN switches and UTMs and also exhibit health status of the device with respect to any internal failure, This configuration shall monitor the critical interconnection status like core switch to Mission Storage or core switch to core switch interconnect etc. User team shall provide the functional requirement of the LAN view.

3) View for Real-time and Offline Service/Application Status – In this view the critical real-time and offline Services will be shown along with system / hardware health and also the service health. Critical service information will be provided to the implementation team for making the required configuration.
4) Security View – This dash board will show the status of critical security function like Antivirus, SIEM, Ansible etc and its running status.
5) Complete LAN view – This will be a discovery view which will list complete topology and every connected device should be visible with in User LAN under this view.
6) The views will be placed in a cyclic view in one screen and in dedicated view in other screens as provisioned by User team.

iv. **SIEM Installation –** Vendor shall carry out the installation of the SIEM solution on 3-server cluster environment/ single node with cold standby server as per requirement and install the agents on all the hosts / VMs. The vendor shall ensure integration of the SIEM with Hosts, VMs, HCI infrastructure, LAN switches, Routers ,Firewall and syslog for detailed view of the events on the network. The SIEM implementation shall cover following reporting capability other than base feature of the products –

1) Failed login attempts
2) Failed authorization attempt
3) Detection of node or traffic other than approve network list
4) Detection of file system commands like rm
5) Network port scan attempt
6) Change in system binary

v. **Proxmox HCI VE Establishment -** Vendor needs to establish three Hyper-Converged Infrastructure (HCI) with Proxmox VE. Each infrastructure shall use 3 Nos of Config -1 Server. Following will be the strategy for deployment –

1) Each Server of a cluster will be deployed in different Rack to ensure cluster survives during a rack power failure
2) The 10G interfaces will be used for cluster heartbeat – as primary and secondary heartbeat channel connected on the core switch network
3) The 1G interface on the servers will be used as node interface.
4) The implementation of the Proxmox VE shall be as per OEM best practice guide. The VM resource allocation also shall be as per best performance recommendations.
5) NSIL/User shall provide the details of the physical host which needs to be migrated on the virtual environment. Vender needs to make detailed plan of the VMs and failover path within each cluster.
6) The success of the configuration and acceptance will be based on the verification of the configuration and after verification of the successful failure of the cluster nodes.
7) Vendor shall engage experienced engineers on the platform for implementation of the cluster.

vi. **Network Behavior Analytics (NBA/NBAD) Installation -** Vendor needs to install the NBA/NBAD collector for three segments of the network as described in the specification and has to ensure complete isolation of the segments via one way technology for data ingestion in NBA collector. Vendor has to ensure that NBA collector should not combine or join three segment of the network and bypass UTM/Firewall rules. However, for analysis purpose, all the logs can be combined and processed. Vendor shall ensure the NBA master controller node will be setup and a dash board will be setup to show the malicious activities detected. The vendor also needs to integrate the alerts in SIEM console. Vendor must ensure that only OEM part number is quoted for implementation support and must ensure yearly one visit by OEM engineer for at-least one weeks' time to tune all the policies and algorithms for better detection.

d. **Security Audit –** During the system implementation phase, vendor will be provided with security control implementation at location as per currently adopted standard. Vendor shall ensure all the security controls are implemented as per guideline and shall create required checklist and verification data after completion of the implementation. While making the implementation of any product, vendor must ensure the OEM recommended hardening standards are adopted for each implementation.

i. NSIL shall depute an expert team to verify the security implementation on the infrastructure and based on the satisfactory findings the implementation will be accepted.

ii. The function of the security implementation will be limited to the platform and capabilities which are delivered as per current contract and additional hardware or software will not be under the scope of implementation.

iii. Vendor shall also note that during onsite support activity, vendor must ensure the security implementation is maintained consistently. User shall conduct yearly security audit by internal expert team as per established standard. All the findings during verification will be with-in the vendor's scope of configuration delivery and shall be completed within one month of official notification.

Appendix 'Y' – UT Display Speifiation

A.0 UT & CDT Time Display

Device Type	:	NTP based UT and CDT Time coder with Display
Make & Model no.	:	

A.1 Specifications

1. Display	:	Seven segment Nine digits display plus +/- segment
2. Time information	:	(a) Universal Time (UT) in Day:Hour:Minute:Second format (b) Count Down Time (CDT) in +/- Hour:Minute:Second format
3. Plus / Minus Sign	:	Off- during UT time information displaying and Plus (+) sign during CDT in counting UP and minus (-) sign during CDT time counting down
4. Input selection	:	Unit shall have Switch to select either UT input or CDT input or suitable provision to be done for displaying either UT or CDT time by reading input time information
5. NTP Over Ethernet	:	(a) Unit should display UT Time coming as Ethernet packets i.e. standard NTP Time output given by NavIC Receiver or GPS receiver (b) Unit should display CDT time coming as Ethernet packets (should support customized packets also) output by SHAR-ISRO CDT Time Format
6. Time Display	:	9 digit ultra-bright 4 inch height 7 segment display (format should be DOY:HH:MM:SS) representing Days (3 digits), Hours (2 digits), Minutes (2 digits) and Second (2 digits), preceded by alpha numeric sign display '+' for Count Up, '-' for Count Down and 'H' for Hold with clear gap (':'colon as separator) between Days, Hours, Minutes and Seconds or

			equivalent letter display 'up' for Count Up , 'dn' for Count Down and 'ho' for Hold.
	7. Time Display LED color	:	Bright Amber / Red colour
	8. Enclosure & Dimension	:	The unit shall be enclosed in a box. The unit dimensions shall be as per design with minimum bezel along the border of the seven segment displays
A.3	**Connectivity**		
	1. Connectivity	:	LAN – 2 ports / LAN-1port & IRIB-G port accordingly unit shall be designed for reading UT and CDT time
	2. Network capabilities	:	Yes, 10/100/1000 Ethernet Base-T RJ-45 connector
	3. EIA/IRIG-B input	:	IRIG-B modulated signal via BNC connector, level 500mV to 10Vpp suitable to output of NavIC / GPS receiver output
A.4	Power Supply	:	Built-in with power 230V +/- 10V AC 50-60Hz

Appendix 'Z' – Onsite Support

a. **Resident Engineer / Onsite Support.**

   i. **Onsite Support Skill1:** Support for unified storage and backup software, Servers and hosts and VMs

   ii. **Onsite Support Skill2:** Support for NMS, Network Switches, Routers and End node connectivity

   iii. **Onsite Support Skill3:** Support for NGFW, SIEM, and Security Implementation in UTM and Security Compliance verification for network elements, server, hosts and VMs and NBA/NBAD

b. **Minimum Skillset Requirement –** The offered onsite resource shall have following minimum skillset requirement criteria –

   i. **Onsite Support Skill1:**
      1) Minimum 3 years onsite experience on offered Storage Product. Experience certificate to be attached.
      2) Certification: Valid RHCSA (Redhat Certified System Administrator)

   ii. **Onsite Support Skill2:**
      1) Minimum 3 years onsite experience on offered Switching and Routing Products. Experience certificate to be attached.
      2) Certification: Valid CCNA (Cisco Certified Networking Associate) Certificate

   iii. **Onsite Support Skill3:**
      1) Minimum 3 years onsite experience on offered NGFW or minimum two years' experience on offered SIEM Product. Experience certificate to be attached.
      2) Certification: Certification on NGFW Advance Security Certification or Certification on any SIEM product

c. **Onsite Engagement –** The offered onsite Engineer shall have following engagements:

   i. The resident engineers shall be positioned at Bhopal Control Center.

   ii. The engineers shall have Weekly 6 days (8 AM to 5 PM) onsite engagement.

   iii. Extended hours support during operational requirement or contingency

   iv. Complimentary off for extended support based on mutual agreement of NSIL/User team

   v. Yearly 15 days official leave will be granted on mutual agreement

   vi. Leaves beyond allowed quota must be compensated with residential engineer of equivalent skill

vii. During release of onsite Engineer there must be three months notice period for knowledge transfer with new resource/onsite Engineer. The existing resource/ onsite Engineer have to ensure all the documents are updated and handed over to the new engineer.

d. **Roles and Deliverables:** The following are the roles and deliverables by the residential engineers –

i. The resident engineers shall be responsible for upkeep of the deployed systems in respective role which includes daily status check, configuration verification, firmware upgrade, fault and failure handling, logging calls with OEM and follow-up, providing logs for trouble-shooting, taking recovery action including fresh installation and replacement of hardware or software etc.

ii. Other than regular health check of the hardware and delivered configuration, the onsite support team shall ensure regular firmware update of the delivered hardware with a planned calendar of update schedule. The update activity will be carried out after due approval of the User/NSIL team. Vendor shall also ensure to implement the security configuration and settings as per existing configuration and also to ensure implementation of security guideline, as per OEM recommended guideline for newly migrated firmware version. During each firmware update cycle, vendor must make a fall back plan in case the upgrade is not complete within scheduled time.

iii. Though the roles are specific for engineers, based on requirement the residents' engineers may need to perform overlapping roles

iv. **Deliverables for Skill1:** Support for unified storage and backup software, Servers and hosts and VMs

1) Daily Verification
   - Status of Storage, Backup server, SAN switch, Tape Library, Servers, VMs, HCI interface and provide health check report on system health
   - Check the backup policy and report backup status
   - Check the status of file system at different servers (central storage and local servers) and report utilization
   - Check the logs of HCI and VMs and report anomalies
2) Weekly Verification
   - Overall report on system heath
   - Pending issues which are not closed last week
   - Update documentation on operation procedures
   - Test recovery of random files in alternate path from latest backups
3) Monthly Reporting
   - Consolidated reporting of the anomalies found and corrective action taken

- Report on parts/spare replacement and highlight pending issues
- Status of firmware or software upgrade (if action is identified)

v. **Deliverables for Skill2:** Support for NMS, Network Switches, Routers and End node connectivity

1) Daily Verification
    - Status of all the network devices in the network both in LAN and WAN (including remote), verification of the device logs and report anomalies
    - Check the status of NMS software , build new services views and alerts as required
    - Status on Port Security 802.1x on network
    - Check for KVM, RKM and Management network status
    - Check for status of data diode, interface and file flow
    - Check for status of Rsync, FTP and other file synchronization process
    - Check for all host connectivity including channel bonding
2) Weekly Verification
    - Configuration backup of all network device
    - Overall report on system heath
    - Link heath report indicating the error rates, downtime and bandwidth utilization
    - Pending issues which are not closed last week
    - Status of network security configuration and compliance report
    - Status of Host security controls as per standard provided
    - Update documentation on operation procedures
3) Monthly Reporting
    - Consolidated reporting of the anomalies found and corrective action taken
    - Report on parts/spare replacement and highlight pending issues
    - Status of firmware or software upgrade (if action is identified)

vi. **Deliverables for Skill3:** Support for NGFW, SIEM, and Security Implementation in UTM, NBA/NBAD and Security Compliance verification for network elements, server, hosts and VMs –

1) Daily Incident analysis, verification and reporting
2) Configuration of new rules
3) Adding new nodes and applications in log collector environment
4) Write parsers, connectors and other programs as necessary to enable integration of new devices with log aggregator
5) Building custom co-relation and notification rules
6) Verification of availability of all data point / collector status
7) Regular tuning of configuration of reduction of false positive notification
8) Whitelisting events and activates for exclusion

9) Configuration for automatic reporting and notification for customized report
10) Integration and monitoring of UTM. NBA/NBAD and antivirus logs
11) Configuration of new data points / collector interface
12) Upgradation and maintenance of log analysis software
13) Incident report preparation and submission as per User/NSIL provided template
14) Daily report –
    - No of open incidents
    - Action Pending from Sysadmin Team
    - Health Check report of all the hardware and software elements in SIEM, UTM fabric and Antivirus and Data Diode
    - Report generation as per NSIL/User provided template
15) Weekly Report–
    - Total No of incidents reported
    - No of open incidents
    - Total No of incidents closed
    - Status of signature update in UTMs and Desktop Antivirus
    - Change in security configuration or settings in Router, Switches, UTMs, Hosts and VMs.
    - Update documentation on operation procedures
16) Monthly Report –
    - Total No of incidents reported
    - No of open incidents
    - Total No of incidents closed
    - Threat categories of the incidents
    - Day wise breakup of incidents
    - Monthly Audit report as per provided Security Standard [This activity will be distributed across entire month and segment wise verification date to be recorded in the report]
    - Status of security patch update

e. **Monthly Review:** The vendor shall identify an account manager role who shall have online / onsite meeting with NSIL, User teamand site engineers on last week of every month to discuss the pending issues and review support deliverable status. The actions with in scope of the deliverables shall be identified and resolved by the vendor. Vendor shall deploy additional skills to ensure specialized maintenance activities is covered by additional temporary skillsets (subject matter experts) as required if any such action is identified during the review.

f. **General terms:**

i. Onsite (resident) support engineer is required for entire contract duration.

ii. Cost for each onsite skill to be quoted separately.

iii. Bio-data and two stamp size photographs of the Resident Engineer to be deployed shall be sent to the Focal Point for records. The Resident Engineer, once approved for the service, should not be changed by Service Provider, without the written concurrence from Focal point

iv. The resident engineer shall be responsible for carrying out all the routine health check, troubleshooting, co-ordination with different OEM in problem solving, firmware/software upgrades and updates storage system configuration changes etc and shall ensure service availability.

v. The resident engineer shall share the configuration and knowledge information with Bhopal and NSIL team periodically.

vi. Vendor shall ensure availability of resident engineer as per the details mentioned above.

vii. The engineer deployed shall reach the work spot well in time and strictly follow the rules and regulations regarding safety and security of NSIL.

viii. The engineer deployed is not authorized to communicate any official information they may come across during & after their working period, to any third party.

ix. Resident Engineer should be present during working hours. If the Service Provider fails to provide the same, Purchaser reserves the right to deduct a proportionate order value from the pending/future bills of the service provider for the period of absence.

x. If a resident Engineer proceeds on leave or leaves the Company, the replacement engineer to be deployed in advance so as to prevent any interruption in services rendered by them. I.e. new (replaced) resident Engineer should have been trained aprior, as an alternate. The same to be conveyed in advance to the Focal point, in writing.

xi. Purchaser reserves the right to seek replacement of the resident engineer if service is found not satisfactory.

xii. Purchaser reserves the right to reject any of the personnel deployed by the Service provider

xiii. The onsite engagement of the resident engineers shall start after completion of the implementation and site acceptance test of the setup.

xiv. The resident engineers must qualify the back ground verification criteria as set by User and NSIL for deployment on site.

xv. The resident engineers must abide by the physical and cyber security guideline as set by NSIL and User.

xvi. The vendor and all the onsite deployed engineers must sign NDA (non-disclosure agreement) with NSIL.

xvii. Except with the written consent of the Authority, the vendor shall not disclose

the contract or any provision, specification, plan, design, pattern, sample or information thereof to any third party.

Appendix 'AA' – Other Technical Terms and Conditions

a. **Common Terms and Conditions:** The following set of specifications shall be met by all the offered items unless explicitly specified.

i. **Installation & System Support –**

1) Vendor should install & commission all the systems as per the configuration at specified user site. The deployment configuration shall be provided during system installation phase.
2) The system implementation document for each element shall be provided by the vendor.
3) The installation shall include unpacking, integration, deployment of the delivered components and as per detailed scope as mentioned in technical specification.
4) Wherever required installation of operating system, upgradation of firmware/IOS, and installation of required device drivers & system libraries shall be carried out by the vendor.
5) Vendor should resolve all issues related to compatibility of hardware, drivers, and other system software with OS.
6) As part of User Acceptance Test (UAT), for all delivered items vendor needs to demonstrate the compliance to the tender specifications for each product. Vendor is required to make required test cases, record the test output and observation and complete the service migration for completion of UAT. Vendor shall provide installation and acceptance report as part of system installation on successful completion of system acceptance by end users.
7) Vendor shall provide required skilled man-power during system installation, service migration and acceptance at user site. The identified skilled man-power shall strictly follow the rules and regulations regarding safety and security of NSIL.
8) At the time of installation and commissioning of the configuration if it is found that some additional hardware accessories or software items with licenses are required to complete the configuration to meet the operational requirement of the configuration which were not included in the vendor's original list of deliverables then vendor is required to supply such items to ensure the completeness of the configuration at no extra cost. Vendor should ensure completeness of the list of deliverables in the offer to avoid such discovery during installation.

ii. **System Support –** Vendor shall provide on-call onsite support for the delivered set of systems during the warranty period. The support shall include onsite activities like failed component replacement, Operating system & device driver installation and configuration, firmware & IOS upgrade, troubleshooting and raising support call with OEM.

1) Vendor shall identify a support engineer in Palayamkottai & Delhi who shall provide on call basis onsite support requirements. The identified engineer shall

reach the work spot well in time and strictly follow the rules and regulations regarding safety and security as per User/NSIL requirement. Further equipment breakup for each location to be provided at the time of PO Placement.

b. **Quality Requirements –**

i. The design and production of critical subsystems like system motherboard, controllers etc., shall be under the control of manufacturer & international quality certified realization process.

ii. All subsystems of the system shall have been selected to achieve optimal performance and high reliability.

iii. The system architecture shall ensure maximum performance for data processing applications. The subsystems, the processor boards, the interconnections among subsystems and the software shall be properly matched to ensure maximum performance.

iv. Systems shall be only from a proven product line from highly reputed manufacturers. The product line shall be an internationally established brand reputed for high quality and with wide acceptance in deployment for mission critical and business critical functions in the industry.

v. The manufacturer of the system shall be in total control of the life cycle (Design, release, support, obsolescence and termination of the critical subsystems like motherboard, controllers etc.,) of the product.

c. **Notes to the Vendor –**

i. Vendor shall submit the following certifications from OEM on OEM's letter head for all deliverables except for SIEM tool, HCI Software, NMS Tool, Microsoft Windows, LAN Cables and Accessories, RHEL -
   1) The vendor is authorized for participating in the bid
   2) The offered hardware is not an obsolete product
   3) The offered hardware / software components will not reach End of Support for atleast seven years from the date of supply
   4) The offered hardware / software component is back to back supported by the OEM during the warranty period

ii. Vendor shall submit the following certifications from OEM on OEM's letter head, wherever applicable (Storage, Servers, Workstations, Laptops, All-in-One, NGFW, Router, Switch, NBA/NBAD etc). The OEM does not have any objection on retention of failed media (Hard disk or NVRAM) at Bhopal & Delhi during warranty replacements

iii. For all items in the list of deliverables offered by the vendor, the

manufacturer's part number should be clearly indicated. Offer of items without clear specification of part number is not acceptable.

iv. Vendor should indicate the part nos. of the deliverable items clearly. The part numbers & description of the items in the offer should match the part numbers & description of the items mentioned in the manufacturer's spec sheets.

v. The part numbers & description of the goods delivered should match the part numbers & description in the offer.

vi. Vendor should carefully consider all the clauses in the specifications and should ensure that their offer is complete in all respects at the time of submission. Complete technical documentation justifying the compliance should be enclosed along with their offer. Offer which are incomplete are liable to be considered noncompliant.

vii. Specifications of the major items have been provided in the enclosed document. In case any additional accessories/ software media/licenses are required to complete the configuration for full functionality and/or better manageability vendor should include such hardware accessories and related software elements or plug-ins with licenses in their offer.

viii. Systems from the manufacturers who primarily assemble systems by getting components/ subsystems from different suppliers and who do not have direct control over the production process/ quality of the items so obtained, will not be acceptable.

ix. Vendor should provide technical brochure from manufacturer for all subsystems to verify the current status (i.e. when released, whether due for replacement/obsolesce) the specification of the subsystems. The technical brochure shall give the details not only for the main system but also for all the subsystems and accessories. Technical brochure shall include details of

1) Functional specification.
2) Hardware & software configuration.
3) Configuration options.
4) Electrical & environmental specification.
5) Safety compliance details.
6) Physical dimension.
7) System test report and reliability metric

x. In case the approval of any Foreign Govt. agency, like US dept. of commerce, is required for the supply of any of the items, vendor should clearly indicate the items requiring such clearance. For such items vendor should obtain strong assurance from the manufacturer regarding their commitment to follow-up through the necessary clearance process. A written assurance to this effect should be enclosed with the technical offer.

d. **Items for delivery at Delhi**

i. List of Items to be transferred to Delhi from Bhopal after completion of UAT on user division request: -

1) Station Computers - 04 nos
2) Edge Switches - 04 nos
3) Routers - 02 nos
4) NGFW (Config-2) - 2 Nos

Post shipment, Vendor should support commissioning of these devices at Delhi.

Chapter 3: Specific Terms and Conditions

3.1 Warranty and Support

a. The warranty shall start from the date of successful completion of installation commissioning and service migration as per scope of the RFP, completion of ATP and delivery of all documents and declaration of go-live at respective sites.

   GO-LIVE: Go live will be scheduled by the authority once the required hardware, software, and services including migration services as desired by authority have been installed by the vendor and are accepted by the authority.

b. The support for the total solution is for a total period of seven years which includes five years of warranty and two years of Comprehensive AMC (CAMC).

c. Comprehensive on-site Warranty (24x7) with the response and resolution times as per the table below for both the supplied hardware and software for a period of five years. The warranty also includes supply and installation of updates and upgrades of the given software including application software, firmware and etc. Tenderer shall quote for warranty & CAMC for the total solution on annual basis for a total period of seven years (5 years warranty and 2 years CAMC).

Response Time	Resolution Time
16 hours	96 hours

d. The vendor shall be responsible to identify the failed component and identify the OEM who will rectify the component, log the call, follow it up and resolve the issue within the stipulated down time allowed.

e. The vendor must have certified skilled, trained and experienced manpower with technical competence on all the quoted products. The Tenderer shall carry out periodic (quarterly) checkups/servicing of the offered solution. The vendor has to produce certification of the skilled manpower on every change of manpower during the seven year period along with police verification certificate.

f. The OEMs shall conduct refresher course at site on Solution and Technology at periodic intervals as per the terms and conditions of the RFP.

g. The vendor shall clearly provide escalation matrix for resolving problems.

h. The Tenderer shall provide certificate along with corresponding part numbers from the OEM confirming the back-to-back service agreement between the Tenderer and the OEM during the entire warranty period of 5 years and plus CAMC for a period of 2 years.

i. Payment to the vendor during the Extended warranty period/ CAMC will be made as per Service Level Agreement. SLA will be decided by mutual consent after order placement as per the scope in the RFP.

3.1.1 Specific Warranty Clauses

i. OEM's support package for on-site 24x7 comprehensive warranty with advance replacement shall be offered for Workstations, Servers, Unified Storage, Tape Library , Backup Server, Network Switches (Core and Edge), UTM /NGFW (including manager, Analyzer and end point protection licenses) and NBA/NBAD

ii. OEM's support package for on-site 8x5 NBD comprehensive warranty with advance replacement shall be offered for All-in-One, Laptops, Monitors, Large Display, Router, RKM, KVM, ATS, NMS Software, NBA/NBAD, Printers,.

iii. Offered OEM's support package shall include warranty for all the items in the BOM.

iv. Wherever applicable persistent media will not be handed over to OEM during replacement process. Vendor shall ensure all persistent media like Disk, Flash etc shall be offered with No Device Return part number in SLA.

v. Warranty / CAMC is required for total 7 years for all items including hardware, software , firmware. If the vendor is not able to provide 7 years support, vendor shall deliver equivalent hardware of same make with equivalent capabilities and migrate the services on the new platform at no extra cost to NSIL/User.

vi. All Windows Operating system and Linux operating system will be covered under one year support with unlimited support calls. Other OS license will be covered as per the specified support with unlimited support calls.

vii. The rate quoted for each item (as indicated in BOM) should include 5 years on-site warranty **unless mentioned otherwise**. A separate break-up should be given for 2 years CAMC for each item.

viii. Manufacturers' support package for Warranty and technical support only should be quoted. The specific part number for such support should be clearly indicated. Vendor shall not replace manufacturer's warranty with their own warranty package.

ix. Wherever OEM supports online listing of supported items in warranty portal, NSIL/User shall verify listing of these hardware/software on online portal with required SLA. Vendor must showcase the listing of the items in OEM portal to ensure support is offered back-to-back.

x. All the equipment's must be register under NSIL/User Email account which will be provided during installation. Vendor shall not register any hardware under their ownership in OEM support portal.

xi. Technical Support to cover the following

1) Access to technical support information for resolving problems, configuration issues, utilities etc.
2) Firmware updates and upgrades & access to device drivers.
3) Access to technical literature relating to the system.
4) Onsite technical support in trouble-shooting and resolution.

3.2 Maintenance

a. The vendor shall carry out periodic (quarterly) checkups/servicing at the respective User sites (including Delhi and Palayamkottai) for the supplied items during warranty period and CAMC period.

b. A SLA (Service Level Agreement) will be signed with vendor for maintenance purpose.

c. In SLA, Tenderer will mention single point of contact for any trouble shooting, call logging, onsite part replacement, periodic checks, health checks etc.

d. In SLA, the response time quoted in Warranty and Support need to be followed for major components.

3.3 CAMC/Extended Warranty - 2 Years (post warranty)

CAMC/Extended Warranty- 2 years (Mandatory, Separate PO)

A Comprehensive AMC for 2 years period w.e.f the date of completion of initial warranty period for entire system, including Spares for Hardware and updates/upgrades for software shall be placed against the requirement. CAMC amount shall be paid yearly basis on completion of yearly period, post standard comprehensive on-site warranty of 5 years for a period of 2 years against the satisfactory performance Certificate issued by concerned engineer/ site in-charge after deducting the penalty amount if any.

Detailed CAMC/Extended Warranty Terms and Conditions:

a. CAMC will be considered as an integral part of supply order and whole unit without exception of any part / accessory, will be covered under CAMC.

b. All the CAMC must be OEM back to back support contract and must be listed in OEM warranty portal.

c. The CAMC involves checking including repair and maintenance of all the equipment and systems purchased under the present Contract agreement.

d. CAMC also includes replacement of defective parts on as and when required basis so that systems are constantly kept in perfect working order as per the scope of this RFP.

e. CAMC also includes supply and installation of updates and upgrades of the given software including application software, firmware, security updates and etc.

f. Earthing and lightening arrestor (required, if any) for equipment and systems purchased shall be maintained by successful bidder/NSIL. Any repair / replacement necessitated due to

lightening is to be covered under the scope of CAMC.

g. The bidder shall render at-least four preventive maintenances to all sites including Delhi and PalayamKottai site in a year. A task list (TODO list) to this effect shall be prepared and submitted before commissioning.

h. Preventive maintenance as per the technical / service / operational manual of the manufacturer, during the CAMC period of 24 months apart from keeping the servicing engineer.

i. There would be no capping on the number of breakdown visits as per terms of the RFP, and they should be undertaken on as and when required basis. Intimation of break down call should be passed on through emails only (The NSIL has to communicate an official email id for registering / booking the breakdown calls).

j. The equipment should be repaired within a specified period from the reporting of the defect. The availability of the equipment should be as per SLA. Beyond that penalty clause will be invoked as per SLA.

k. All the support terms and clauses as mentioned in (initial) warranty clause is applicable in the scope of CAMC deliverable. .

3.4 Penalty Clause.

During the CAMC period the equipment are to be kept in working condition and provide availability as per SLA.

The methodology to calculate the %age of availability for the component will be specified in the SLA:

$$\%\text{ age availability} = \frac{A - (\text{Break down hours} - \text{Hours lost due to delay in giving Break down information- resolution time as per RFP} - \text{Preventive Maintenance Downtime as per SLA})}{A} \times 100$$

where A = No. of days in a quarter x 24 hrs.

Terms and conditions of Payment:

a. No advance payment shall be made during CAMC/extended warranty period.

b. The payment of CAMC/ extended warranty charges is payable on annual basis as per SLA.

c. Submission of Bill: CAMC/ extended warranty bill shall be submitted on annual basis.

d. CAMC from the date of commencement of contract is for two years depending on the performance of the firm and compliance of terms & Conditions.

e. Breakdown to be computed only in case of operational breakdown. For example, in case of

components in HA mode, breakdown to be computed only when both components are down.

No	Availability	Penalty
1	>97%	No penalty
2	Between 95% and 97%	5% of CAMC value for the quarter for the component– Excluding Manpower charges
3	Between 90% and 95%	10% of CAMC value for the quarter for the component - Excluding Manpower charges
4	Between 80% and 90%	20% of CAMC value for the quarter for the component - Excluding Manpower charges
5	<80%	50% of CAMC value for the quarter for the component - Excluding Manpower charges

3.5 Delivery Terms & Schedule

The vendor shall deliver all deliverable items within 32 weeks from placement of order as per the payment terms. Entire Transportation of all items in to be done by the seller for delivery to the sites without any additional cost. The schedule break up shall be provided with the proposal. The duration of ATP and fixing of any problem should be within above specified duration. No extension in delivery schedule will be granted without a valid reason approved by NSIL. There will be regular review of the completed activities of vendor by NSIL from time to time and vendor should submit weekly update reports. Further, the vendors should note that:

a. During implementation and warranty support period, if it is observed that any of the supplied components of the system (software and hardware) are not able to handle load or its performance is not able to meet the functional requirements/ technical specifications given in the Tender, the vendor at its own cost shall replace that component (software or hardware) with higher end equipment or provide additional Hardware (along with Operating System)/software components/Licenses for meeting the technical specifications and user requirements.

b. The vendor is responsible for resolving any operational issues.

c. It is mandatory that in case of hardware failure, the repair and maintenance has to be provided by vendor as per mutually agreed terms and conditions.

3.6 Implementation Specific Terms and Conditions

a. All the hardware specifications mentioned in this RFP are the required minimum, however higher or better specifications would be preferable.

b. Component furnished shall be complete in every respect with all mountings, fittings, fixtures and standard accessories normally provided with such components and/or needed for erection, completion and safe operation of the components as required by applicable codes though they may not have been specifically detailed in the technical specification, unless included in the list of exclusions. All similar standard components/parts of similar standard components provided shall be inter-changeable with one another.

c. The thermal engineering aspect should be considered during placing equipment in rack for efficient cooling.

d. The methodology of cabling and installation work to be adopted to ensure minimum damage to the existing structure of the building. Any damage caused by vendor to the existing flooring/ walls/paint etc. shall be rectified by the vendor.

e. The Vendor shall be responsible for providing all materials, components, and services as specified to fulfil the intent of ensuring operability, maintainability, and reliability of the complete component covered under this RFP.

f. The Vendor shall also be responsible for deputing qualified personnel for installation, testing, commissioning and other services under his scope of work as per this specification. All required tools for completing the scope of work as per the specification is also the responsibility of the selected bidder. A standard toolkit for maintenance to be provided for use by the service engineer including vacuum cleaner, blower, temperature-controlled soldering station, network cabling kit, network cable maintenance tool kit, screwdriver kit, LAN tester, optical fibre power meter etc. required for effective maintenance of the equipment.

g. The Vendor shall perform the services and carry out its obligations with all due diligence, efficiency and economy in accordance with generally accepted professional techniques and practices and shall observe sound management practices and employ appropriate advance technology and safe methods.

h. The Vendor shall furnish complete, well-fabricated and reliably operating and secure systems. Design and selection of component and software shall be consistent with the requirements of long-term trouble-free operation with highest degree of reliability and maintainability.

i. All components shall be constructed to operate safely without undue heating, vibration, wear, corrosion, electromagnetic interference or similar problems and all software shall be proven, tested and reliable. The necessary compliance document

and test reports shall be provided.

j. All interconnecting cables required to connect the communication component shall be furnished. All cables shall be fully assembled connector pre-terminated and factory tested as part of overall system checkout. Cables shall be neatly and properly tied up and dressed using appropriate cable hangers and Velcro bands. All the cables, connectors, sockets, panels etc. shall be labeled for identification purpose.

k. Component shall be guaranteed for operation over the following AC power range to be made available 240 V AC +/-10%, 50 Hz +/-5%. Reliable over voltage and over current protection circuits shall be provided in the component power supply units. The component power supply units shall be self-protecting and also protect connected components against interference, noise, voltage dips and surges and impulses that may be present in the mains power supply sources.

l. Proper earthing arrangement shall be made as per industry standards for the offered equipment. Including earthing pits and earthing strip laying with resistance less than 1 ohm.

3.7 Site Readiness and Preparation

a. The Vendor shall carry out the site inspection within four weeks of the placement of PO.

b. The Vendor shall assess the requirements of total power, UPS, floor space, number of racks and Air conditioning during site inspection and the same shall be intimated to NSIL in writing.

3.8 Installation, Integration and Commissioning

a. Vendor shall install and commission the systems as per existing configuration in consultation with the Authority.

b. System installation, commissioning is the responsibility of the Vendor, his System Integrator and OEM. Vendor/SI's responsibility to co-ordinate with OEM.

c. The Vendor through his System Integrator, has to install the Server configuration, Network components and other supplied hardware/software/supplies as per buyer's requirement.

d. It is the responsibility of the vendor to resolve any performance related issues in consultation with the Authority.

e. The scope of the installation covers the complete installation and commissioning of the complete solution including all the hardware and software items offered as part

of this tender.

f. The upgradation of the system is to be undertaken in the live environment and therefore availability of all the required hardware along with required expertise is to be ensured by the vendor.

g. Tender shall provide site-planning guide for all the subsystems quoted.

3.9 Training

a. The Vendor through his System Integrator has to provide detailed training through an OEM certified Engineer immediately after ATP commences. Thereafter, every year, training shall be provided for the total solution by an engineer trained by the OEM, during the warranty and CAMC period at a common site as decided by User/ NSIL.

b. Training to be offered on RHEL Administration, Windows Server Administration, Storage Administration, Network Switch Administration, Backup software and Tape Library operations, Security Solution, UTM, NBAD, SIEM, Hypervisors etc. along with major components including other software/hardware items as supplied by the vendor.

c. The training shall be provided in a structured format for a period of minimum seven working days for min. 10 people during the support period (7 years).

3.10 Acceptance Test procedure (ATP)

a. Vendor shall prepare the detailed ATP document and the following points shall be included in the ATP document. The document shall be prepared in advance and submitted to Authority for inspection purpose. The demonstration procedure shall be mentioned in document with necessary tool and commands.

b. A connectivity diagram of all equipment offered in the solution and functional test covering all the equipment in and integrated mode shall be demonstrated.

c. Vendor shall conduct a 72 Hours burn-in test for all equipment and necessary logs files shall be generated.

d. Vendor shall provide a list of all equipment as BOM (Bill of Material) and the specifications mentioned in the RFP.

e. Site inspection should be done before actual delivery.

f. Vendor should demonstrate servers/software components/system/supplies with standard utilities as per service utilization requirement.

g. The storage controller fail-over test has to be demonstrated. HA mode has to be

demonstrated for all equipment supplied/configured in HA.

h. The structure cabling performance i.e. jitter free communication has to be demonstrated using standard tools.

i. Vendor to note that site is an operational facility and all migration and system installation activity to be executed in coordination with the operational activities with minimal downtime or zero downtime wherever possible.

j. Team shall be ready to work during 24X7 to complete the project as per the schedule.

k. ATP includes all the scope defined in “Appendix ‘X’ – One time Implementation and Documentation” along with acceptance of other services/supplies as per the scope of the RFP.

Chapter 4: Special Terms and Conditions for the RFP

4.1 Specific Specifications Clause

The following specification clause will from part of the contract placed on successful Bidder - The Vendor guarantees to meet the specifications as per RFP/tender and to incorporate the modification to the existing design configuration to meet the specific requirement of the Buyer service as per modifications/requirements recommended as per the scope of the RFP/tender after the maintenance evaluation trials. All technical literature and drawing shall be amended as the modification by the seller before supply to the Buyer. Seller, in consultation with the Buyer, may carry out technical upgradation / alterations in the design, drawings and specifications due to change in manufacturing procedures, indigenization or obsolescence. This will, however, not in any way, adversely affect the end specifications of the equipment. Changes in technical details, drawings repair and maintenance techniques along with necessary tools as a result of up-gradation/alterations will be provided to the buyer free of cost within 15 days of affecting such up-gradation/alternations.

4.2 OEM Certificate.

OEM certificate for bidding and warranty is mandatory. In case the Bidder is not the OEM, the agreement certificate with the OEM for sourcing the spares shall be mandatory. However, where OEMs do not exist, minor aggregates and spares can be sourced from authorized vendors subject to quality certification. Authorised distributions of OEM may be given performance subject to price reasonability to terms & condition of RFP.

4.3 Earliest Acceptable Year of Manufacture.

Items supplied are to be of latest year of manufacture. Quality/Life certificate will need to be enclosed with the Bill.

4.4 Buyer Furnished Equipment.

The buyer will not provide any equipment to Seller at his expense.

4.5 Transportation.

All items required to be supplied and installed at user sites as well as at all other locations listed in technical specifications are to be transported by the Vendor at no extra cost to the buyer.

4.6 Packing and Marking.

The following Packing and Marking clause will form part of the contract placed on successful Bidder –

a. The Vendor shall provide packing and preservation of the equipment and spares/goods contracted so as to ensure their safety against damage in the conditions of land, sea and air transportation, transhipment, storage and weather hazards during transportation, subject to proper cargo handling. The Vendor shall

ensure that the stores are packed in containers, which are made sufficiently strong, and with seasoned wood. The packing cases should have hooks for lifting by crane/fork lift truck. Tags with proper marking shall be fastened to the special equipment, which cannot be packed.

b. The packing of the equipment and spares/goods shall conform to the requirements of specifications and standards in force in the territory of the OEM's country.

c. Should any special equipment be returned to the Vendor by the Buyer, the latter shall provide normal packing, which protects the equipment and spares/goods from the damage of deterioration during transportation by land, air or sea. In this case the Buyer shall finalize the marking with the Seller.

4.7 Quality.

The quality of the stores delivered according to the present Contract shall correspond to the technical conditions and standards valid for the deliveries of the same stores for in Seller's country or specifications enumerated as per RFP and shall also include therein modification to the stores suggested by the Buyer. Such modifications will be mutually agreed to. The Seller confirms that the stores to be supplied under this Contract shall be new and shall incorporate all the latest improvements and modifications thereto and spares of improved and modified equipment are backward integrated and interchangeable with same equipment supplied by the Seller in the past if any. The Seller shall supply an interchangeability certificate along with the changed part numbers wherein it should be mentioned that item would provide as much life as the original item.

4.8 Quality Assurance.

Seller would provide the Standard Acceptance Test Procedure (ATP) with delivery of equipment. Buyer reserves the right to modify the ATP on mutual consent basis. Seller would be required to provide all test facilities his premises for acceptance and inspection by buyer. The details in this regard will be coordinated during the negotiation of the contract. The item should be of the latest manufacture, conforming to the current production standard and having 100% defined life at the time of delivery.

4.9 Technical Documentation

Full technical specifications and literature (both hard and soft copies) must be provided for all the quoted items including sub-items. This includes, but not limited to, operation manual, installation documents, user document, technical specification and design document, system maintenance documents, checklist for maintenance etc.