



**RAILTEL CORPORATION OF INDIA LIMITED**  
(A Govt. of India Undertaking, Ministry of Railways)

Expression of Interest for Selection of Partner from Empaneled Business Associates  
or OEMs or OEM's authorized partner/distributor

for

“Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT  
Hardware & Software for five years at MRSAC under Maha-BHUMI Project”

EOI No: RailTel/WR/BPL/MRSAC/EOI/2024-25/32

Dated 07<sup>th</sup> February 2025

Plot No. 17, 1st Floor, Raghunath Nagar, Near Shahpura Police station,  
Bhopal MP-462039

## EOI NOTICE

RailTel Corporation of India Limited, Plot No. 17, 1st Floor, Raghunath Nagar, Near Shahpura Police Station,  
Bhopal MP - 462039

EOI No: RailTel/WR/BPL/MRSAC/EOI/2024-25/32

Dated 07<sup>th</sup> February 2025

RailTel Corporation of India Ltd., (here after referred to as “RailTel”), publishes EOI to select suitable partner among RailTel’s Empaneled BA / OEMs / OEM’s authorized partner / distributor(s) for work of “Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under Maha-BHUMI Project”

The details are as under:

1	Last date for submission of Bid response Packet against EOIs by bidders	11 <sup>th</sup> February 2025 at 16:00 Hours
2	Opening of Bid response packet of EOIs	11 <sup>th</sup> February 2025 at 16:30 Hours
3	Number of copies to be submitted for scope of work	One
4	EMD Amount	<p>Rs. 50,00,000/- (Rupees Fifty Lakh Only) (in form of BG) (Refer Annexure-7)</p> <p>Empaneled BA may submit the EMD in two parts. Detailed as under –</p> <p>1. Token EMD – Rs. 5 Lakhs in form of BG or cash transfer in account of RailTel (Bank details given at Annexure – 6)</p> <p>2. The balance amount of advertised EMD by BA will be submitted one day before final submission of bid to customer. Remaining EMD value Rs. 45 Lakh in form of BG or cash transfer in account of RailTel (Bank details given at Annexure – 6)</p>
5	Tender Fees & Processing Fees	Rs. 15,000/-

The EMD in form of BG should be in the favor of RailTel Corporation of India Limited payable at Mumbai.

Partner needs to submit BG with all details as per Annexure – 7.

Against Tender fee and processing fee deposition, online payment details like UTR No. date and Bank detail to be submitted along with the technical proposal.

### **RailTel Bank Details:**

**1. Name of the Bank - Union Bank of India**

**2. Account No. - 317801010036605**

**3. IFSC Code - UBIN0531782**

**4. Branch name – Mahalaxmi Branch**

Eligible Business Associates / OEMs / authorized partner or distributor(s) of OEM are directed to do all communications related to this Invitation for EoI document / documentation, through the following officials:

**Level:1**

Name: Sh. Anand Kumar

Position: Jt. General Manager/Marketing

Email: [anandnkn@railtelindia.com](mailto:anandnkn@railtelindia.com)

Contact: +91-9004444107

**Level:2**

Name: Sh. Pavan Kumar Bhargava

Position: ED/TM/Bhopal

Email: [pavan@railtelindia.com](mailto:pavan@railtelindia.com)

**Note:**

1. Empaneled BA's / OEMs / authorized partner or distributor(s) of OEMs are required to submit soft copy (password protected PDF) against EOI response separately for Technical and Financial response through an e-mail at [bpltooffice@railtelindia.com](mailto:bpltooffice@railtelindia.com) duly signed by Authorized Signatory with Company seal and stamp. **The size of both the files should not exceed 20 Mb.**
2. **The OEMs need not be prior empaneled Business Associates, given their proven technical prowess. However,** The EOI response is invited from eligible **Empaneled BA's / Partners of RailTel only in case of participation by Business Associates.**
3. The password will be sought at the time of opening of the bid response packet.
4. All the documents must be submitted with proper indexing and page no.
5. This is an **exclusive arrangement with empaneled business associate/OEMs/authorized partner or distributor(s) of OEM of RailTel for fulfilling the end customer requirements.**
6. Selected partner's authorized signatory has to give an undertaking that, they will not submit directly or indirectly their bids and techno-commercial solution / association with any other organization once selected through this EOI (before and after submission of bid to prospective organization by RailTel). This undertaking has to be given with this EOI Response.
7. **Transfer and Sub-letting.** The Business Associate/OEMs/authorized partner or distributor of OEM has no right to give, bargain, sell, assign or sublet or otherwise dispose of the Contract or any part thereof.  
As well as to give or to let a third party take benefit or advantage of the present Contract or any part thereof.

## 1. Introduction about RailTel

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

RailTel has approximately 70000 kms of OFC along the protected Railway tracks. The transport network is built on high capacity DWDM and an IP/ MPLS network over it to support mission critical communication requirements of Indian Railways and other customers. RailTel has Tier-III Data Center in Gurgaon and Secunderabad hosting / collocating critical applications. RailTel is also providing Telepresence as a Service (TPaaS), where a High- Definition Video Conference facility bundled with required BW is provided as a Service.

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

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

Licenses & Service portfolio:

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



a) Carrier Services

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

b) Enterprise Services

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

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

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

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

e) Retail Services – Rail Wire

Rail Wire: Triple Play Broadband Services for the Masses. RailTel has unique model of delivering broadband services, wherein local entrepreneurs are engaged in delivering & maintaining broadband services and up to 66% of the total revenues earned are shared to these local entrepreneurs in the state, generating jobs and revitalizing local economies. On date RailTel is serving approx. 4,00,000 subscribers on PAN Indian basis. RailTel can provide broadband service across– Government PSU or any organization's officers colonies and residences.

## 2. Project Background and Objective of EOI

RailTel intends to participate in the work for “Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under Maha-BHUMI Project”

RailTel invites EOIs from RailTel’s Empaneled Partners/OEMs/authorized partner or distributor of OEMs for the selection of suitable partner for participating in above mentioned work for the agreed scope work. The empaneled partner/OEMs/authorized partner or distributor of OEMs is expected to have excellent execution capability and good understanding customer local environment.

## 3. Scope of Work

The scope of work is to “Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under Maha-BHUMI Project” as per there requirement. The above scope of work is indicative, and the detailed scope of work will be shared after the completion of the EOI process.

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

Special Note: RailTel may retain some portion of the work mentioned in the end organization RFP, where RailTel has competence so that overall proposal becomes most winnable proposal. Scope of Work and payment terms shall be on a back-to-back basis as per the end customer RFP.

## 4. Response to EOI guidelines

### 4.1 Language of Proposals

The proposal and all correspondence and documents shall be written in English in password protected PDF file through an email (size of email should not exceed 20Mb) to [bpltooffice@railtelindia.com](mailto:bpltooffice@railtelindia.com)

### 4.2 RailTel’s Right to Accept/Reject responses

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

### 4.3 EOI response Document

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

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

#### 4.4 Period of Validity of bids and Bid Currency

Bids shall remain valid for 180 days from the date of submission.

#### 4.5 Bidding Process

The bidding process as defined in para 9.

#### 4.6 Bid Earnest Money (EMD)

- 4.6.1 The Business Associate shall furnish a sum as given in EOI Notice via online transfer from any scheduled bank in India in favor of “RailTel Corporation of India Limited” along with the offer.
- 4.6.2 Offers not accompanied with valid EOI Earnest Money Deposit shall be summarily rejected.
- 4.6.3 In case of Business Associate’s offer is selected for bidding, a BA has to furnish Earnest Money Deposit (for balance amount as mentioned in the customer’s Bid as and if applicable) for the bid to RailTel. The selected Business Associate shall have to submit a Bank Guarantee against EMD in proportion to the quoted value/scope of work to RailTel before submission of bid to end customer, as and if applicable.
- 4.6.4 EMD and Tender Fees will be deposited in the form of Online Bank Transfer.
- 4.6.5 The validity of such EMD shall be maintained till the finalization of end Customer RFP/Tender i.e. award of order and till submission of Performance Guarantee of requisite value required by end customer on back-to-back basis.
- 4.6.6 Return of EMD for unsuccessful Business Associates: Final EMD of the unsuccessful Business Associate shall be returned without interest after completion of EOI process (i.e. after pre-bid agreement is signed with the selected partner)
- 4.6.7 Return of EMD for successful Business Associate: Final Earnest Money Deposit (balance proportionate EMD) if applicable of the successful bidder will be discharged / returned as promptly as possible after the receipt of RailTel’s EMD/BG from the Customer and or on receipt of Security Deposit Performance Bank Guarantee as applicable (clause no. 4.7) from Business Associate whichever is later.
- 4.6.8 Forfeiture of Token EOI EMD or EMD (balance proportionate EMD) and or Penal action as per EMD Declaration:
  - 4.6.8.1 The EOI EMD may be forfeited and or penal action shall be initiated if a Business Associate withdraws his offer or modifies the terms and conditions of the offer during validity period.

#### 4.7 Security Deposit / Performance Bank Guarantee (PBG)

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

4.7.2 As per work share arrangements agreed between RailTel and Business Associate the PBG will be proportionately decided and submitted by the selected Business Associate.

#### 4.8 Last date & time for Submission of EOI response

EOI response must be submitted to RailTel at the email address specified in the preamble not later than the specified date and time mentioned in the preamble.

#### 4.9 Modification and/or Withdrawal of EOI response

EOI response once submitted will be treated, as final and no modification will be permitted except with the consent of the RailTel. No Business Associate shall be allowed to withdraw the response after the last date and time for submission.

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

#### 4.10 Clarification of EOI Response

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

#### 4.11 Period of Association / Validity of Agreement

RailTel will enter into agreement with selected bidder with detailed Terms and conditions.



## 5. Pre-Qualification Criteria for Bidding Business Partner of RailTel

S No.	Particulars	Criteria for Tender Package
		(Mandatory Compliance & Document Submission)
1	The SI Bidder must be incorporated and registered in India under the Indian Companies Act 1956 or 2013, or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 and should have been in operation in India for a minimum of five years as on 31.03.2024. The SI Bidder must be registered with appropriate authorities for all applicable statutory duties/taxes.	1. Copy of certificate of Incorporation / Registration under Companies Act 1956/2013 (for Indian companies) 2. Copy of GST certificate 3. Copy of PAN Card 4. Valid Empanelment letter (LOI) issued by RailTel
2.	SI Bidder must have average annual turnover of INR 75 crores from IT/ITES business for last three audited financial years (i.e. FY 2021-22, 2022-23, 2023-24) And SI Bidder should have a positive net worth as on bid submission date.	1. Copy of audited profit and loss account and balance sheet for latest three financial years (FY 2021-22, 2022-23, 2023-24) 2. Certificate from Statutory Auditor with UDIN and stamp for both average annual turnover and positive net worth.
3.	SI Bidder should have established/implemented Data Centre projects for Central / State Governments, PSUs, PSEs in India in the last five (5) years: a. One project of value INR 70 Crores or more; OR b. Two projects each having minimum value of INR 60 Crores or more; OR c. Three projects each having minimum value of INR 40 Crores or more The Data Centre project consisting of Supply, Installation, Testing and Commissioning (SITC) of IT components such as server, storage, backup system, network, cyber security equipment for the Data Centre; Non-IT components including installation, commissioning of any of these Electrical Distribution & Lighting, DG sets, Precision AC/ Chiller Plant, UPS System, Fire Detection & suppression system, Access Control and CCTV, BMS System. Note: Bidder's in-house projects setup will not be considered.	1. Work orders & Completion certificate 2. Datacentre Completion certificates on the client letter head for the completed project also signed by the authorized signatory.
5.	SI Bidder should have experience of setting up and managing NOC operations, Service Desk for Central / State Governments / PSUs /PSEs in India in last 5 years Note: Bidder's in-house projects setup will not be considered	For on-going projects: 1. Work orders & Agreement highlighting scope of work. 2. In progress certificates on the client letter head of the projects For completed projects: 1. Work orders & Agreement highlighting scope of work. 2. Completion certificates on the client letter head of the projects/Self-Certificate by the authorised signatory
6.	The SI Bidder shall provide all the three Certifications valid at the time of bidding: • ISO 9001:2015 or latest certification • ISO 20000:2018 or latest certification • ISO 27001:2013 or latest certification	Copies of the valid certificates in the name of the SI.
7.	As on date of submission of the proposal, the SI Bidder, shall not be blacklisted / debarred by any State / Central Government Department or Central /State PSUs / PSEs.	The SI Bidder Undertaking as per the format on company letter head.
8.	Furnishing of the Power of Attorney	Power of Attorney executed by the SI Bidder in favor of the duly Authorized signatory, certifying him/her as an authorized signatory for the purpose of this Tender.

<b>Sr. No.</b>	<b>Pre-Qualification Criteria</b>	<b>Documents required substantiating pre-qualifying criteria</b>
1.	Implementation of HCI solution, x86server virtualization.	Proof of capabilities in the form of completion certificate for atleast one successfully complemented implementation at Central/State government agencies, departments, PSUs, etc.
2.	Backup Storage & Software	Proof of capabilities in the form of completion certificate for atleast one successfully complemented implementation at Central/State government agencies, departments, PSUs, etc.
3.	Active Networking Components-Core switch, Access switch, Enterprise Network Firewall, Router: Should provide as per specifications	Proof of capabilities in the form of completion certificate for atleast one successfully complemented implementation at Central/State government agencies, departments, PSUs, etc.
4.	Security – Threat Management – HIPS, EDR: Should provide as per specifications	Proof of capabilities in the form of completion certificate for atleast one successfully complemented implementation at Central/State government agencies, departments, PSUs, etc. EDR: Solution should have 5+ Patents for Malware & Ransomware Protection. Solution should be 100% Make in India Product. The Solution should have OPSWAT Certification & AV-Test Certification for Endpoint security
5.	Undertaking must be submitted from OEM that the products being quoted by the SI are of latest model/version and will not be declared as “end-of-support”, “end-of-sale”, “end-of-service” by the respective OEM (Original Equipment Manufacturer) within 5 years of publishing of this tender.	Undertaking from OEM meeting this criterion
6.	Undertaking must be submitted from OEM that the support including spares, patches, upgrades/updates, etc. for the quoted products shall be available for next 5 years from the date of successful installation & acceptance of the project.	Undertaking from OEM meeting these criteria

<b>S No.</b>	<b>Annexures</b>	<b>Description</b>
1	<b>Annexure 1</b>	<b>Covering Letter:</b> Self-certification duly signed by authorized signatory on company letter head.
2	<b>Annexure 2</b>	The Bidder should agree to abide by all the technical, commercial & financial conditions of the end customer RFP for which EOI is submitted.
		Self-certification duly signed by authorized signatory on company letter head.
3	<b>Annexure 3</b>	An undertaking signed by the Authorized Signatory of the company to be provided on letter head. The Bidder should not have been blacklisted / debarred by any Governmental / Non-Governmental Organization in India as on bid submission date.
4	<b>Annexure-4</b>	Format for Affidavit to be uploaded by BA along with the tender documents.
5	<b>Annexure-5</b>	Non-disclosure agreement with RailTel.
6	<b>Annexure-6</b>	Bank Mandate
7	<b>Annexure-7</b>	Bank Guarantee Format
8	<b>Annexure-8</b>	Tender Document
9	<b>Annexure - 9</b>	Power of Attorney and Board Resolution in favor of one of its employees who will sign the Bid Documents.
10	<b>Additional Documents to be Submitted</b>	Technical Proposal with overview of the project with strength of the Partner.
11	<b>Annexure-10</b>	BOQ of the RFP document. Price Bid Format to be submitted in separate password protected pdf.

## 6. Bidder's Profile

The bidder shall provide the information in the below table:

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

## 7. Evaluation Criteria

- 7.1 The Business Associates are first evaluated on the basis of the Pre-Qualification Criteria as per clause 5 above.
- 7.2 The Business Associate who meets all the Pre-qualification criteria, their price bid will be evaluated. The Lowest (L1) price bidder will be selected and entered into agreement with for delivery of the work on back-to-back basis for the agreed scope of work.
- 7.3 RailTel reserves the right to further re-negotiate the prices with eligible L1 bidder. Selected bidder must ensure the best commercial offer to RailTel to offer the most winnable cost to customer.
- 7.4 RailTel also reserves the right to accept or reject the response against this EOI, without assigning any reasons. The decision of RailTel is final and binding on the participants. The RailTel evaluation committee will determine whether the proposal/ information is complete in all respects and the decision of the evaluation committee shall be final. RailTel may at its discretion assign lead factor to the Business associate as per RailTel policy for shortlisting partner against this EOI. RailTel also reserves the right to negotiate the price with the selected bidder.
- 7.5 All General requirement mentioned in the Technical Specifications are required to be complied. The solution proposed should be robust and scalable.

## 8. Payment terms

- 8.1 RailTel shall make payment to selected Business Associate after receiving payment from Customer for the agreed scope of work. In case of any penalty or deduction made by customer for the portion of work to be done by BA, same shall be passed on to Business Associate.
- 8.2 All payments by RailTel to the Partner will be made after the receipt of payment by RailTel from end Customer organization.

## 9. SLA

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

## 10. Other Terms and Conditions

Any other terms and conditions in relation to SLA, Payments, PBG etc. will be as per the PO/agreement/Work Order/RFP of the end customer.

Note: Depending on RailTel's business strategy RailTel may choose to work with Partner who is most likely to support in submitting a winning bid.

**Annexure 1**

**COVERING LETTER**  
(To be submitted on company letter head)

EoI Reference No:

Date :

To,

RailTel Corporation of India Ltd.  
Plot No. 17, First Floor,  
Raghunath Nagar,  
Near Shahpura Thana,  
Bhopal, M.P. - 462039

Dear Sir,

SUB: Participation in the EoI process

Having examined the Invitation for EoI document bearing the ref. no. \_\_\_\_\_ released by your esteemed organization, we, undersigned, hereby acknowledge the receipt of the same and offer to participate in conformity with the said Invitation for EoI document.

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

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

We hereby Submit EMD amount of Rs. \_\_\_\_\_ issued vide \_\_\_\_\_ from Bank \_\_\_\_\_.

Authorized Signatory

Name

Designation

Self-Certificate  
(To be submitted on company letter head)

EoI Reference No:

Date:

To,

RailTel Corporation of India Ltd.  
Plot No. 17, First Floor,  
Raghunath Nagar,  
Near Shahpura Thana,  
Bhopal, M.P. - 462039

Dear Sir,

**Sub: Self Certificate for Tender, Technical & other compliances**

- 1) Having examined the Technical specifications mentioned in this EOI & end customer tender, we hereby confirm that we meet all specification.
- 2) We agree to abide by all the technical, commercial & financial conditions of the end customer RFP for which EOI is submitted (except pricing, termination & risk purchase rights of the RailTel). We understand and agree that RailTel shall release the payment to selected BA after the receipt of corresponding payment from end customer by RailTel. Further we understand that in case selected BA 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 BA.
- 3) We agree to abide by all the technical, commercial & financial conditions of the end customer's RFP for the agreed scope of work for which this EOI is submitted.
- 4) We hereby agree to comply with all OEM technical & Financial documentation including MAF, Technical certificates/others as per end-to-end requirement mentioned in the end customer's RFP. We are hereby enclosing the arrangement of OEMs against each of the BOQ item quoted as mentioned end customer's RFP. We also undertake to submit MAF and other documents required in the end Customer organization tender in favour of RailTel against the proposed products.
- 5) We hereby undertake to work with RailTel as per end customer's RFP terms and conditions. We confirm to submit all the supporting documents constituting/ in compliance with the Criteria as required in the end customer's RFP terms and conditions like technical certificates, OEM compliance documents.
- 6) We understand and agree that RailTel is intending to select a BA who is willing to accept all terms & conditions of end customer organization's RFP for the agreed scope of work. RailTel will strategies to retain scope of work where RailTel has competence.

- 7) We hereby agree to submit that in case of being selected by RailTel as BA for the proposed project (for which EOI is submitted), we will submit all the forms, appendix, relevant documents etc. to RailTel that is required and desired by end Customer well before the bid submission date by end customer and as and when required.
- 8) We hereby undertake to sign Pre-Bid Agreement and Non-Disclosure Agreement with RailTel on a non-judicial stamp paper of Rs. 100/- in the prescribed Format.

Authorized Signatory

Name & Designation



**Annexure 3:**

**Undertaking for not Being Blacklisted/Debarred**  
(To be submitted on Company Letter Head)

To,

RailTel Corporation of India Ltd.  
Plot No. 17, First Floor,  
Raghunath Nagar,  
Near Shahpura Thana,  
Bhopal, M.P. - 462039

Subject: Undertaking for not Being Blacklisted/Debarred

We, \_\_\_\_\_ Company Name \_\_\_\_\_, having its registered office at  
\_\_\_\_\_ address \_\_\_\_\_ hereby declares that that the Company  
has not been blacklisted/debarred by any Governmental / Non-Governmental organization in India  
for past 3 Years as on bid submission date.

Date and Place

Authorized Signatory's Signature:

Authorized Signatory's Name and Designation:

Bidder's Company Seal:

**Annexure 4:**

**Format of Affidavit**  
**FORMAT FOR AFFIDAVIT TO BE UPLOADED BY BA ALONGWITH THE EOI**  
**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 BA) \*\*

I..... (Name and designation) \*\* appointed as the attorney/authorized  
signatory of the BA (including its constituents),

M/s.....(hereinafter called the BA) for the purpose of the EOI  
documents for the work of ..... as per the EOI No.  
..... of (RailTel Corporation of India Ltd.), do hereby solemnly affirm and state on the  
behalf of the BA including its constituents as under:

1. I/we the BA (s), am/are signing this document after carefully reading the contents.
2. I/we the BA(s) also accept all the conditions of the EOI and have signed all the pages in confirmation thereof.
3. I/we hereby declare that I/we have downloaded the EOI documents from RailTel website [www.railtelindia.com](http://www.railtelindia.com). I/we have verified the content of the document from the website and there is no addition, no deletion or no alternation to be content of the EOI document. In case of any discrepancy noticed at any stage i.e. evaluation of EOI, execution of work or final payment of the contract, the master copy available with the RailTel Administration shall be final and binding upon me/us.
4. I/we declare and certify that I/we have not made any misleading or false representation in the forms, statements and attachments in proof of the qualification requirements.
5. I/we also understand that my/our offer will be evaluated based on the documents/credentials submitted along with the offer and same shall be binding upon me/us.
6. I/we declare that the information and documents submitted along with the EOI by me/us are correct and I/we are fully responsible for the correctness of the information and documents, submitted by us.
7. I/we undersigned that if the certificates regarding eligibility criteria submitted by us are found to be forged/false or incorrect at any time during process for evaluation of EOI, it shall lead to forfeiture of the EOI EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the BA) \*\* ..... and all my/our constituents understand that my/our constituents understand that my/our offer shall be summarily rejected.

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

DEPONENT SEAL AND SIGNATURE  
OF THE BA

#### VERIFICATION

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

DEPONENT SEAL AND SIGNATURE  
OF THE BA

Place:  
Dated:

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

### **NON-DISCLOSURE AGREEMENT**

This Non-Disclosure Agreement (this “**Agreement**”) is made and entered into on this \_\_\_\_ day of \_\_\_\_, 2024 (the “**Effective Date**”) at \_\_\_\_\_. By and between

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

And

\_\_\_\_\_) (CIN: \_\_\_\_\_), a company duly incorporated under the provisions of Companies Act, \_\_\_\_\_ having its registered office at \_\_\_\_\_, (hereinafter referred to as '**\_\_\_\_\_**'),

which expression shall unless repugnant to the context or meaning thereof, deem to mean and include its successors and its permitted assignees of OTHER PART

RailTel and \_\_\_\_\_ shall be individually referred to as “Party” and jointly as “Parties”

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

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

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

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

**Permitted Use.**

Receiving Party shall:

hold all Information received from Disclosing Party in confidence; use such Information for the purpose of evaluating the possibility of entering into a commercial arrangement between the Parties concerning such Information; and restrict disclosure of such Information to those of Receiving Party’s officers, directors, employees, affiliates, advisors, agents and consultants (collectively, the “**Representatives**”) who the Receiving Party, in its reasonable discretion, deems need to know such Information, and are bound by the terms and conditions of (1) this Agreement, or (2) an agreement with terms and conditions substantially similar to those set forth in this Agreement.

The restrictions on Receiving Party's use and disclosure of Information as set forth above shall not apply to any Information that Receiving Party can demonstrate: is wholly and independently developed by Receiving Party without the use of Information of Disclosing Party; at the time of disclosure to Receiving Party, was either (A) in the public domain, or (B) known to Receiving Party; is approved for release by written authorization of Disclosing Party; or is disclosed in response to a valid order of a court or other governmental body in the India or any political subdivision thereof, but only to the extent of, and for the purposes set forth in, such order; provided, however, that Receiving Party shall first and immediately notify Disclosing Party in writing of the order and permit Disclosing Party to seek an appropriate protective order.

(c) 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.

**Designation.**

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

written or other tangible form, such Information is clearly marked as proprietary or confidential when disclosed to Receiving Party; or oral or other intangible form, such Information is identified as confidential or proprietary at the time of disclosure.

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

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

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

**Return or Destruction of Information.**

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

termination of this Agreement; expiration of this Agreement; or  
Receiving Party's determination that it no longer has a need for such Information.

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

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

**Notice.**

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

by personal delivery, when delivered personally; by overnight courier, upon written verification of receipt; or by certified or registered mail with return receipt requested, upon verification of receipt.

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

Attn: \_\_\_\_\_

Address: \_\_\_\_\_

Phone:

Email.:

Attn: \_\_\_\_\_

Address: \_\_\_\_\_

Phone:

Email:

### **Term, Termination and Survivability.**

Unless terminated earlier in accordance with the provisions of this agreement, this Agreement shall be in full force and effect for a period of \_\_\_\_years from the effective date hereof.

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

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

In respect to Information provided to it during the Term of this agreement, shall survive and continue even after the expiry of the term or termination of this agreement; and not apply to any materials or information disclosed to it thereafter.

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

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

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

### **Settlement of Disputes:**

The parties shall, at the first instance, attempt to resolve through good faith negotiation and consultation, any difference, conflict or question arising between the parties hereto relating to or concerning or arising out of or in connection with this agreement, and such negotiation or consultation shall begin promptly after a Party has delivered to another Party a written request for such consultation.

In the event of any dispute, difference, conflict or question arising between the parties hereto, relating to or concerning or arising out of or in connection with this agreement, is not settled through good faith negotiation or consultation, the same shall be referred to arbitration by a sole arbitrator.

The sole arbitrator shall be appointed by CMD/RailTel out of the panel of independent arbitrators maintained by RailTel, having expertise in their respective domains. The seat and the venue of arbitration shall be New Delhi. The arbitration proceedings shall be in accordance with the provision of the Arbitration and Conciliation Act 1996 and any other statutory amendments or modifications thereof. The decision of arbitrator shall be final and binding on both parties. The arbitration proceedings shall be conducted in English Language. The fees and cost of arbitration shall be borne equally between the parties.

### **CONFIDENTIALITY OF NEGOTIATIONS**

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

## **REPRESENTATION**

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

## **ASSIGNMENT**

Neither this Agreement nor any of the rights, interests or obligations under this Agreement shall be assigned, in whole or in part, by operation of law or otherwise by any of the Parties without the prior written consent of each of the other Parties. Any purported assignment without such consent shall be void. Subject to the preceding sentences, this Agreement will be binding upon, inure to the benefit of, and be enforceable by, the Parties and their respective successors and assigns. its Affiliates to advise their Representatives, contractors, subcontractors and licensees, of the obligations of confidentiality and non-use under this Agreement, and shall be responsible for ensuring compliance by its and its Affiliates' Representatives, contractors, subcontractors and licensees with such obligations. In addition, each Party shall require all persons and entities who are not employees of a Party and who are provided access to the Confidential Information, to execute confidentiality or non-disclosure agreements containing provisions no less stringent than those set forth in this Agreement. Each Party shall promptly notify the other Party in writing upon learning of any unauthorized disclosure or use of the Confidential Information by such persons or entities.

## **NO LICENSE**

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

## **RELATIONSHIP BETWEEN PARTIES:**

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

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

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



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

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

\_\_\_\_\_:

RailTel Corporation of India Limited:

By\_\_\_\_\_

By\_\_\_\_\_

Name:

Name:

Title:

Title:

Witnesses

## Annexure-6 – Bank Mandate



**Mahalaxmi Branch  
Mahalaxmi Chambers  
22, Bhulabhai Desai Road  
MUMBAI: 400 026**

**Tel. No. No.23512895 / 23517234 Fax No.23516948**

**LT No:MAH/RCIL/2010**

**Date: 21/10/2010**

To,  
The Sr. Manager (Finance)  
Railtel Corporation Of India Limited  
Mahalaxmi, Mumbai

Dear Sir,

Sub-: Bank Details For your collection account.

We are in receipt of your letter no. RCIL/WR/Fin/Bank Matters dated 20.10.2010  
Requesting bank details for your collection account no. 317801010036605. Details are below:-

Account No.- 317801010036605

A/c Name- Railtel WR collection A/c

Bank Name- UNION BANK OF INDIA

Branch name- Mahalaxmi, branch

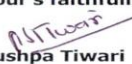
Branch address- 22, bhulabhai desai Road, Mahalaxmi chambers,  
Mahalaxmi, Mumbai-400026

IFSC Code- UBIN0531782

Swift Code- UBININBBLOP

Thanking You

Your's faithfully

  
Pushpa Tiwari  
Manager



**Bank Guarantee for Earnest Money Deposit**

(To be stamped in accordance with stamp act)

Ref: Bank Guarantee #

Date -

Principle Executive Director,  
Western Region  
RailTel Corporation of India Limited,  
Mahalaxmi, Mumbai.

Dear Sir,

Whereas (hereinafter called "the SI") has submitted its tender offer dated dd/mm/yyyy for providing services for tender "Selection of System Integrator (SI) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project"

KNOW ALL MEN by these presents that we \_ of \_ (herein after called the Bank) are bound up to (here in after called "the Department ") in the sum of \_ for which payment well and truly To be made to the said Purchaser, the Bank bind sit self, its successors and assigns by these presents; sealed with the Common Seal of the Said Bank this \_ day of \_.

THE CONDITIONS of this obligation are:

- If the SI/bidder withdraws its tender during the period of tender validity specified by the Tenderer on the Tender Form; or
- If the SI/bidder, having been notified of the acceptance of its tender by the Department during the period of tender validity:

Fails or refuses to execute the contract Form if required; or

Fails or refuses to furnish the Performance Security, in accordance with the instruction given in tender document.

We undertake to pay the Department up to the above amount upon receipt of its first written demand, without the Department having to substantiate its demand, provided that in its demand the Department will note that the amount claimed by it is due to owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee is valid up to 180 days from last date of bid submission and shall be governed and construed in accordance with Indian Laws.

Date:

Place:

**Beneficiary Bank Detail as below –**

1. Name of the Bank - Union Bank of India
2. IFSC Code - UBIN0531782
3. Branch name – Mahalaxmi Branch

**Name of signatory:**

**Designation:**

**Email ID:**

**Contact No.:**

**Bank Common Seal:**

**Annexure- 8**

**Tender Document**

RFP – Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under Maha-BHUMI Project.



## **Request for Proposal (RFP)**

Selection of System Integrator (S.I) for Supply, Installation, Testing,  
Commissioning of IT Hardware & Software for five years at MRSAC under  
MahaBHUMI Project

**RFP Number:** MRSAC/SI/01/2025

**Issued on:** 29.01.2025

## Contents

<b>1</b>	<b>Glossary .....</b>	<b>5</b>
<b>2</b>	<b>Definitions.....</b>	<b>9</b>
<b>3</b>	<b>Invitation for Proposal .....</b>	<b>10</b>
	<i>MAHARASHTRA REMOTE SENSING APPLICATION CENTRE .....</i>	<i>10</i>
	<i>Confidentiality .....</i>	<i>11</i>
	<i>Disclaimer .....</i>	<i>11</i>
	<i>Important Dates / Information – Fact Sheet.....</i>	<i>13</i>
<b>4</b>	<b>Introduction &amp; Background .....</b>	<b>14</b>
4.1	About MRSAC.....	14
4.2	Project Background .....	14
4.3	Broad Objectives of Project.....	14
<b>5</b>	<b>Pre-qualification Criteria.....</b>	<b>15</b>
5.1	Pre-qualification Criteria for System Integrator: .....	15
5.2	Pre-Qualification Criteria for OEMs: .....	17
<b>6</b>	<b>Instructions to SIs .....</b>	<b>18</b>
6.1	Purpose of Bid Document.....	18
6.2	Cost of Bid Document.....	18
6.3	Completeness of Bid Document .....	18
6.4	Proposal Preparation Cost.....	18
6.5	Bid Cover Letters .....	18
6.6	Power of Attorney .....	18
6.7	Queries to be sent (No Pre-bid meeting) .....	19
6.8	Amendments to Bid Document.....	19
6.9	Rights to Terminate the Process.....	19
6.10	Language of Bids.....	20
6.11	Bid Submission Format.....	20
6.12	Online Bid Submission.....	20
6.13	Procedure for Submission of Bids.....	21
6.14	Two Envelope Bid System .....	21

6.15	Supporting Documents for Bid .....	21
6.16	Earnest Money Deposit (EMD) and Refund.....	22
6.17	Evaluation Process.....	23
6.18	Opening of Bid.....	23
6.19	Evaluation of Technical Bids .....	23
6.20	Guidelines for composition of Technical Proposal .....	29
6.21	Period of Validity of Bids .....	30
6.22	Clarification of Bids.....	30
6.23	Non-Material Non-Conformities.....	31
6.24	Opening of Commercial Bid .....	31
6.25	Evaluation of Commercial Bids and Award Criteria .....	32
6.26	Terms and Conditions.....	32
6.27	Rights to Accept/Reject any or all Proposals .....	33
6.28	Fraud and Corruption.....	33
6.29	Notifications of Award and Signing of Contract .....	34
6.30	Performance Bank Guarantee.....	34
6.31	Stamp Duty.....	34
<b>7</b>	<b>Scope of the Work: .....</b>	<b>35</b>
7.1	Introduction:.....	35
	<i>Existing Infrastructure:</i> .....	38
7.2	Supply, Installation, Commissioning, Operations & Maintenance of IT Infrastructure: .....	38
7.3	Detailed Technical Specifications .....	39
a.	Delivery & Installation: .....	84
b.	Technical Terms & conditions.....	86
c.	Warranty & Technical Support: .....	87
d.	Post Warranty Maintenance Support: .....	87
e.	Ownership of the provided accessories.....	88
f.	Other Terms & conditions: .....	88
g.	Capacity Building and Training.....	88
h.	Site Engineers (Project Personnel) .....	89
i.	Setting up Help Desk Services .....	91
j.	Testing.....	92
k.	Product Documentation .....	92
l.	System Monitoring & Compliance to SLA .....	93

m.	Exit Management.....	95
n.	Implementation and adherence to IT policies as defined by MRSAC.....	95
o.	System Architecture for On Premise items at MRSAC: .....	96
<b>8</b>	<b>Implementation Plan &amp; Payment Schedule:.....</b>	<b>97</b>
8.1	Implementation Plan .....	97
8.2	Project Milestones.....	97
8.3	Payment Schedule .....	100
<b>9</b>	<b>Service Level Agreement .....</b>	<b>101</b>
9.1	Introduction.....	101
9.2	Definitions .....	101
9.3	Technical Terms and Conditions:.....	105
9.4	Implementation Phase Service Level Agreement (SLA) Criteria with the System Integrator .....	108
9.5	Post-Implementation Phase Service Level Agreement (SLA) Criteria with the System Integrator.....	108
<b>10</b>	<b>Formats for Pre-Qualification and Technical Bid Submission .....</b>	<b>111</b>
<b>11</b>	<b>Formats for the Technical Bid Response .....</b>	<b>119</b>
<b>12</b>	<b>Annexures.....</b>	<b>129</b>
	Annexure 1: List of Hardware/Software Required .....	129
	Annexure 2: Governance Schedule.....	130
	Annexure 3: Draft Contract Agreement .....	132
	Annexure 4: Formats for the Commercial Bid Response.....	150



## 1 Glossary

Abbreviation	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AD	Active Directory
ADC	Application Delivery Controller
API	Application Program Interface
ATP	Acceptance Test Procedure
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BLD	Blade Server
BOM	Bill of Material
CD	Compact Disk
CIFS	Common Internet File System
CLI	Command Line Interface
CNC	Command and Control Servers
COS	Class of Service
CPU	Central Processing Unit
DB	Database
DC	Data Centre
DDOS	Distributed Denial of Service
DDR	Double Data Rate
DHCP	Dynamic Host Control Protocol
DMZ	Dematerialized zone.
DNS	Domain Name Service
DP	Discovery Protocol
DR	Disaster Recovery
DRAM	Dynamic Random-Access Memory
DSCP	Differentiated services code point
DVD	Digital Video Disk
ECC	Error-correcting code
EIA	Electronic Industries Alliance
EVPN	Ethernet VPN
FC	Fibre channel
FCOE	Fibre channel over Ethernet
GB	Giga byte
GBE	Giga byte Ethernet
GHZ	Giga hertz
GRE	Generic routing encapsulation
GSLB	Global Server Load Balancing
GUI	Graphical user interface
H/W	Hardware

HBA	Host Bus Adapter
HDD	Hard disk drive
HSRP	Hot Standby Router Protocol
HTML	Hyper Text Mark-up Language
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet group management protocol
IOPS	Input output per second
IP	Internet protocol
IPS	Intrusion prevention system
ISCSI	Internet Small Computer Systems Interface
ISD	Input Service Distributor
ISIS	Intermediate System-to-Intermediate System protocol
KVM	keyboard, video, mouse
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LDAP	Local directory access protocol
MAF	Manufacturer authorization form
MD5	Message digest
MGDDS	Maharashtra geo-spatial digital database system
MITM	Man in the Middle of Attack
MPLS	Micro protocol label switching
MPXIO	Multipathing input output
MRSAC	Maharashtra Remote Sensing Application Centre
MS	Microsoft
MSDP	Multicast source discovery protocol
NAS	Network Attached Storage
NFS	Network File System
NGFW	Next generation firewall
NGIPS	Next generation intrusion prevention system
NIC	Network Interface Card
NLSAS	Near line storage Serial-attached SCSI
NMS	Network Management Service
NSPOF	No single point of failure
OEMS	Original equipment manufacturer.
OS	Operating System
OSPF	Open Shortest Path First
OVM	Oracle virtual machine
PBG	Performance Bank Guarantee
PBR	Policy-Based Routing
PDF	Portable data format
PDU	Power Data Unit
PO	Purchase Order
POE	Power on Ethernet

PPP	Point to point protocol
PSU	Public sector Unit
QOS	Quality of service
QSFP	Quad Small Form-factor Pluggable
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant array of independent disk
RAM	Random access memory
RBAC	Role based access control
RD	Read
RDP	Remote Desktop Protocol
REST	Representational state transfer
RFP	Request for proposal
RIP	Routing Information Protocol
RJ	Registered Jack
RMON	Remote Monitoring Configuring Remote Monitoring (RMON)
RPM	Revolution Per Minutes
RTT	Round-Trip Time (RTT)
S/W	Software
SAN	Storage Area Network
SD	Secure Digital Card
SDS	Software Defined Storage
SIEM	Security information and event managers
SI	System Integrator
SLA	Service level agreement
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SOW	Scope of work
SPAN	Switched Port Analyzer
SQL	Structured query language
SSD	Solid State Drives
SSH	Secure shell
SSM	Source specific multicast
STP	Spanning tree protocol
SVI	Switch Virtual Interface
TACACS	Terminal Access Controller Access Control System
TB	Tera byte
TCP	Transmission control protocol
TFTP	Trivial file transfer protocol
UDP	Universal data protocol
URL	Uniform resource locator
USB	Universal serial bus
VLAN	Virtual local area network
VM	Virtual machine

VPN	Virtual private network.
VRF	Virtual routing and forwarding
VRRP	Virtual router redundancy protocol
VXLAN	Virtual Extensible LAN
WAN	Wide area network
WR	Write
WRED	Weighted Random Early Detection

## 2 Definitions

- i. **“Competent Authority”** means, Director, MRSAC, the authority to which the power is delegated by or under these Rules, Delegation of Financial Power Rules or any other general or special orders issued by the GoverningBody of MRSAC.
- ii. **“Financial Year”** means the year beginning on the 1st of April and ending on the 31st of March of the followingyear.
- iii. **“Successful Bidder”** is the bidder chosen by the project owner to receive award of the contract for performing the saidscope of work.
- iv. **“System Integrator”** is an organization that specializes in bringing together component subsystems into a wholeand ensuring that those subsystems function together, a practice known as system integration.
- v. **“Net worth”** is measured as paid-up capital plus free reserves
- vi. **“Department”** means Maharashtra Remote Sensing Application Centre (MRSAC)
- vii. **“IT Infrastructure”** means hardware & software including networking components (active & passive) provided by the bidder.
- viii. **“SI”** or **“Respondent”** or **“Bidder”** is the entity which submits bid as per this RFP

### 3 Invitation for Proposal

#### **MAHARASHTRA REMOTE SENSING APPLICATION CENTRE**

(Autonomous Body of Planning Department, Govt. of Maharashtra)

VNIT Campus, S.A. Road, Nagpur-10 Tel. No. (0712)- 2220086 / 2238576

Online Tenders (e-tender) in Two Bids (Qualifying Bid & Commercial Bid) are invited by the Director, Maharashtra Remote Sensing Application Centre, Nagpur, on Govt. of Maharashtra <https://mahatenders.gov.in/> from interested bidders for “Selection of System Integrator (SI) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project”.

The bidder must be Company having valid registration in India. Tender form, conditions, specifications, methodology and deliverables etc., can be downloaded from the tendering portal of <https://mahatenders.gov.in/> after entering the details of payment of INR 15000 Tender Form Fees (Non-refundable) and payments towards Bid Security of INR 50 Lakhs to be remitted online only. The original Bid Security must be submitted to MRSAC before the last date and time of submission of tender.

The other details can be viewed and downloaded online directly from website of the Govt. of Maharashtra <https://mahatenders.gov.in/> from date of tender published.

Right to accept or reject any or cancel all tenders, without assigning any reason thereof, is reserved by the Director, MRSAC.

Director  
MRSAC, Nagpur

-----

Bidders are advised to study this tender document carefully before submitting there at the cost of bidder proposals in response to the Tender Notice and visit MRSAC Nagpur for site verification, if required. Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document (and clarification/corrigendum issued subsequently, if any) with full understanding of its terms, conditions, and implications.

## Confidentiality

Information shared to the bidders through this document is confidential in nature. Any further circulation of this information, without prior permission of MRSAC is prohibited and would attract punishment/penalties.

This Tender document is not transferable.

## Disclaimer

1. Maharashtra Remote Sensing Application Centre, an autonomous body under Planning Department, Government of Maharashtra has issued this Request for Proposal (hereinafter referred to as “RFP”) for Selection of System Integrator (SI) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project on such terms and conditions as set out in this RFP document, including but not limited to the Technical Specifications set out in different parts of this RFP document.
2. This RFP has been prepared with an intention to invite prospective Applicants / Bidders and to assist them in making their decision of whether to submit a proposal. It is hereby clarified that this RFP is not an agreement, and the purpose of this RFP is to provide the bidder(s) with information to assist them in the formulation of their proposals. This RFP document may not be appropriate for all persons, and it is not possible for MRSAC to consider the investment objectives, financial situation, and particular needs of each bidder.
3. MRSAC has taken due care in preparation of information contained herein. However, this information is not intended to be exhaustive. Interested parties are required to make their own inquiries and shall be required to submit the same in writing (as part of pre-bid queries). This RFP includes statements, which reflect various assumptions and assessments arrived at by MRSAC in relation to the Project. Such assumptions, assessments, and statements do not purport to contain all the information that each bidder may require.
4. This RFP is not an agreement by and between MRSAC and the prospective bidders or any other person. The information contained in this RFP is provided on the basis that it is non-binding on MRSAC, or any of its respective officers, employees, agents, or advisors. MRSAC makes no representation or warranty and shall incur no liability under any law as to the accuracy, reliability, or completeness of the information contained in the RFP document. Each bidder is advised to consider the RFP document as per his understanding and capacity. The bidders are also advised to do appropriate examination, enquiry and scrutiny of all aspects mentioned in the RFP document before bidding. Bidders are encouraged to take professional help of experts on financial, legal, technical, taxation, and any other matters/sectors appearing in the document or specified work. Bidders are also requested to go through the RFP document in detail and bring to notice of MRSAC any kind of error, misprint, in accuracies, or omission in the document. MRSAC reserves the right not to proceed with the project, to alter the timetable reflected in this document, or to change the process or procedure to be applied. MRSAC also reserves the right to decline to discuss the Project further with any party submitting a proposal.
5. No reimbursement of cost of any type shall be paid to persons or entities submitting a Proposal. The bidder shall bear all costs arising from, associated with, or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by MRSAC, or any other costs incurred in connection with or relating to its Bid.

6. The issue of this RFP does not imply that MRSAC is bound to select and pre-qualify Bids for Bid Stage or to appoint the Selected bidder, as the case may be, for the project and MRSAC reserves the right to reject all or any of the Bids without assigning any reasons whatsoever.
7. MRSAC may, in its absolute discretion but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP.
8. MRSAC, its employees and advisors make no representation or warranty and shall have no liability (for any cost, damage, loss or expense which may arise from or is incurred or suffered on account of anything contained in this RFP or otherwise, including but not limited to the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to be part of this RFP or arising in any way with eligibility of bidder for participation in the Bidding Process) towards any Applicant or bidder or a third person, under any law, statute, rule, regulation or tort law, principles of restitution or unjust enrichment or otherwise.
9. MRSAC also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any bidder upon the statement contained in this RFP.
10. Interested parties, after careful review of all the clauses of this 'Request for Proposal', are encouraged to send their suggestions in writing to MRSAC. Such suggestions, after review by MRSAC may be incorporated into this 'Request for Proposal' as a corrigendum which shall be uploaded onto the e-tender website (<https://mahatenders.gov.in/> and MRSAC website).



## Important Dates / Information – Fact Sheet

*Table 1 Important Dates/Information*

#	Information	Details
1.	Project Name	Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project
2.	Tender reference No	e-Tender Notice No: MRSAC/SI/01/2025
3.	Tender Fee	15,000/-
4.	Earnest Money Deposit	50 Lakhs
5.	Bid Validity Period	180 Days
6.	Performance Bank Guarantee	5% of the Contract Value.
7.	Performance Security Validity Period	3 months after expiration of all the Contractual Obligations.
8.	Availability of Tender Document online	29.01.2025
9.	Last date for submission of written queries for clarifications (No Pre-Bid meeting will be organized)	06.02.2025 till 05:30 PM
10.	Last date (deadline) for uploading the bid on e-Tendering website	18.02.2025 till 03:00 PM
11.	Date of online opening of Pre-Qualification cum Technical proposals received Online	19.02.2025 at 03:00 PM
12.	Date of opening of financial proposals received Online	–To be Communicated Later
13.	Contact Person for queries	Administrative Officer
14.	Addressee and Address for the EMD to be submitted	Administrative Officer Maharashtra Remote Sensing Application Centre (MRSAC), VNIT Campus, South Ambazari Road, Nagpur, Maharashtra - 440010
15.	Email ID:	adm-mrsac@mrsac.gov.in
16.	Submission Type	Open, e-Tendering system

## **4 Introduction & Background**

### **4.1 About MRSAC**

The advance technique of remote sensing using multipurpose satellite imageries of earth surface obtained through Indian remote sensing satellites as well as foreign satellites is being widely used for generation of resources database. Based on it, developmental plans of natural resources are being prepared to achieve the objective of sustainable development. Recognizing the potentials of Remote Sensing Technology Scope of its application in the state and infrastructure facilities established by the DoS, the Govt. of Maharashtra established Maharashtra Remote Sensing Applications Centre (MRSAC) in 1988, under the administrative control of Planning Department, at Nagpur to cater the needs of the state.

### **4.2 Project Background**

Recently, Planning Department, Govt. of Maharashtra has declared MRSAC as the “State Nodal Agency” for procurement of satellite imageries on behalf of Government of Maharashtra and share it with user departments, after processing, through Maharashtra Geo-spatial Digital Database System–(MGDDS) under MahaBHUMI project. MRSAC is, also, entrusted with the role of custodian of Remote sensing and GIS information on central server and develop a decision support system for use of RS/GIS database in State.

In this connection, MRSAC intends to upgrade its existing IT Infrastructure on premise for creation of Image Base library using high resolution Satellite data & feature abstraction in various thematic maps, leading to creation of a Geo- Spatial Database. A GIS based decision support system for user departments is also envisaged in this project. Accordingly, MRSAC will be generating voluminous data (Peta bytes) in the next 5 (five) years. In order, to meet this requirement, the capacity of IT infrastructure for MahaBHUMI needs to be planned appropriately and shall include (but not limited to) latest IT hardware/software to create virtual machines using Hypervisor and Server/Desktop virtualization technology.

### **4.3 Broad Objectives of Project**

The objectives of this project are to ensure the following:

- i. Providing easy, anywhere, and anytime access to users (both information & transactional) to ensure reliability, efficiency, transparency, and accountability.
- ii. Delivery to all user departments with RS and GIS services at state/district/taluka/town level in electronic form through state portals by using the MGDDS.
- iii. Development of RS and GIS applications to be hosted at the MRSAC for delivery of services.
- iv. Extensive capacity building and training of field level functionaries to ensure smooth migration to electronic delivery of RS and GIS services and phasing out manual delivery of services.

## 5 Pre-qualification Criteria

The bidder must possess the requisite experience, strength, and capabilities in providing the services necessary to meet the requirements, as described in this RFP. The bidder must also possess the technical know-how and the financial wherewithal that would be required to successfully complete the scope of work mentioned in this RFP, for the entire period of the contract. The bids must be complete in all respect and should cover the entire scope of work as stipulated in the bid document.

The minimum eligibility criteria that should be satisfied by the bidder(s) is mentioned below. The formats for the Pre-qualification documents are given in Annexures of this RFP, unless specified otherwise. It is mandatory to submit the documents in support of the above eligibility criteria and otherwise, bidder(s) is likely to be disqualified if it fails to provide any of the specified documents.

### 5.1 Pre-qualification Criteria for System Integrator:

*Table 2 Pre-Qualification Criteria for SI*

Sr. No.	Pre-Qualification Criteria	Single SI	Documents required substantiating pre-qualifying criteria
1	The SI should be:  A Company registered under the Indian Companies Act, 1956 or 2013, with registered offices in India. OR A partnership firm registered under Indian Partnership Act, 1932.	Mandatory	Copy of Certificate of Incorporation/Registration Certificate
2	The SI should be single partner/firm registered in India. No consortium of firms is allowed.	Mandatory	Copy of Certificate of Incorporation/Registration Certificate
3	The SI should be in existence for minimum of 7 years as on bid submission date in India and should have functional office in Maharashtra state with dedicated technical & maintenance staff in Maharashtra Office.	Mandatory	Certificate of Commencement/ Certificate of Incorporation AND Proof of office in Maharashtra State as on bid submission date
4	Cumulative annual turnover of the last three audited financial years (FY2021-22, FY2022-23, FY2023-24) from IT/ITES Services	Minimum INR 50 Crores	Audited Balance sheets and Profit & Loss account statements of the SI/bidder for each of the last three audited financial years FY2021-22, FY2022-23, FY2023-24 AND CA certificate clearly stating the turnover from IT/ITES Services
5	The SI must have a positive net worth as on date of bid submission.	Mandatory	Latest Certificate duly signed by Statutory Auditor of the SI/bidder or Certified Chartered Accountant specifying the net worth of the SI.

6	The SI should possess the following valid certification as on bid submission date: ISO 9001, 20000, 27001 and CMMI Level 5	Mandatory	Copy of valid certificate issued by the competent authority as on date of bid submission
7	The SI should have at least 5 nos. of experienced professionals (Network/Security/Systems/storage/server) certified professionals on its payroll with B.E./ B.Tech./ MCA degree or equivalent as on bid submission date, having experience in Hardware & Software installation, commissioning, and maintenance services.	Mandatory	Self-Certified letter by the HR head on the letter head of the SI, duly signed by the Authorized Signatory
8	<p>The SI, in last 7 years (as on bid submission date) should have undertaken:</p> <p>One Project of on-premises project of Server/Storage/Network/Endpoint or Security setup* with Single project value of at least INR 17 crore involving infrastructure implementation in India.</p> <p style="text-align: center;">OR</p> <p>Two projects of value not less than INR 9 crores</p> <p style="text-align: center;">OR</p> <p>Three Projects of value not less than INR 6 crores</p> <p>*Note: On-premises project means supply, installation, testing, commissioning, and maintenance (for at least 5 or 3 years) of IT Hardware/Infrastructure including networking/ compute/software licenses</p>	Mandatory	PO copy, Invoice Copy/Work order (WO)/Contract document(s) or Completion certificate(s) or Go Live certificate from client or Project Citation in the attached format. All above supporting documents must mandatorily mention the value of project and duration of the contract.
9	The SI must submit the OEM authorization letter for all products to be supplied specifically for this tender.	Mandatory	Manufacturer Authorization Form (MAF) (in the given format) from the respective OEM(s) which clearly mentions this tender reference number. The original documents whenever required should be submitted along with hard copy of tender.
10	The SI should not be blacklisted and/or debarred by any State or Central Government agency/Government undertaking/PSUs/UT, registered private entity and/or by any of the competent courts, in India, for any default at time of submission of bid against this RFP	Mandatory	Undertaking duly signed by the Authorized Signatory of the SI and should be duly notarized. The original documents whenever required should be submitted along with hard copy of tender.
11	The SI must have valid Goods & Service Tax registration in India & PAN/TAN registration.	Mandatory	Proof of valid Goods & Service Tax Registration in India & Copy of PAN/TAN Card

## 5.2 Pre-Qualification Criteria for OEMs:

*Table 3 Pre-Qualification criteria for OEMs*

Sr. No.	Pre-Qualification Criteria	Documents required substantiating pre-qualifying criteria
1.	Implementation of HCI solution, x86server virtualization.	Proof of capabilities in the form of completion certificate for atleast one successfully complemented implementation at Central/State government agencies, departments, PSUs, etc.
2.	Backup Storage & Software	Proof of capabilities in the form of completion certificate for atleast one successfully complemented implementation at Central/State government agencies, departments, PSUs, etc.
3.	Active Networking Components-Core switch, Access switch, Enterprise Network Firewall, Router: Should provide as per specifications provided in section 7.3	Proof of capabilities in the form of completion certificate for atleast one successfully complemented implementation at Central/State government agencies, departments, PSUs, etc.
4.	Security – Threat Management – HIPS, EDR: Should provide as per specifications provided in section 7.3	Proof of capabilities in the form of completion certificate for atleast one successfully complemented implementation at Central/State government agencies, departments, PSUs, etc.  EDR: Solution should have 5+ Patents for Malware & Ransomware Protection. Solution should be 100% Make in India Product. The Solution should have OPSWAT Certification & AV-Test Certification for Endpoint security
5.	Undertaking must be submitted from OEM that the products being quoted by the SI are of latest model/version and will not be declared as “end-of-support”, “end-of-sale”, “end-of-service” by the respective OEM (Original Equipment Manufacturer) within 5 years of publishing of this tender.	Undertaking from OEM meeting this criterion
6.	Undertaking must be submitted from OEM that the support including spares, patches, upgrades/updates, etc. for the quoted products shall be available for next 5 years from the date of successful installation & acceptance of the project.	Undertaking from OEM meeting these criteria

**Note:** All documents submitted by the SI must be in the given format only unless a format is not provided in this RFP. Documents in any other formats shall be rejected. SIs must quote the products which fully comply with the technical specifications of the proposed products else the bids shall be rejected. OEM(s) should not be blacklisted and/or debarred by any State or Central Government agency/Government undertaking/PSUs/UT, registered private entity and/or by any of the competent courts, in India for any reason.

## **6 Instructions to SIs**

### **6.1 Purpose of Bid Document**

This document provides information to enable the bidder(s) to understand the broad requirements to submit their "Bids".

### **6.2 Cost of Bid Document**

The Cost of Tender document is INR 15,000/- (non-refundable) which shall be paid online only.

### **6.3 Completeness of Bid Document**

Bidder(s) are advised to study all instructions, forms, terms, requirements, and other information in the Bid Documents carefully. Submission of bid shall be deemed to have been done after careful study and examination of the Bid Document with full understanding of its implications. The response to this Bid Document should be full and complete in all respects. Failure to furnish all required information, submission of a proposal not substantially responsive in every respect will be at the bidder's risk and may result in rejection of the bid.

The bidder(s) must possess the technical know-how and the financial ability that would be required to successfully provide the services sought by Department, for the entire period as mentioned in this Bid Document. The Bid must be complete in all respects, conform to all the requirements, terms and conditions and specifications as stipulated in this Bid Document.

### **6.4 Proposal Preparation Cost**

The bidder(s) shall be responsible for all costs incurred in connection with participation in this process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal, in providing any additional information required by Department to facilitate the evaluation process, and in negotiating a definitive Contract or all such activities related to the bid process. Department will in no case be responsible or liable for such costs, regardless of the conduct or outcome of the bidding process.

This Bid Document does not commit Department to award a contract or to engage in negotiations. Further, no reimbursable cost may be incurred in anticipation of award. All materials submitted by the bidder(s) shall become the property of the Department and may be returned at its sole discretion.

### **6.5 Bid Cover Letters**

Each bidder(s) shall submit a completed Bid Covering Letter in accordance with the format specified in this bid document (wherever applicable), one each for the Pre-qualification/Technical bid folder and Commercial bid folder.

### **6.6 Power of Attorney**

Each bidder(s) shall submit a scanned and digitally signed copy of power of attorney executed on non-judicial Stamp Paper of Rs. 500/- duly notarized; indicating that the person(s) signing the bid has the authority to sign the Bid and thus that bid is binding upon the SI during the full period of its validity. The original copy of the

power of attorney document should be submitted to MRSAC along with hardcopy of the tender within three working days after the bid submission deadline.

## 6.7 Queries to be sent (No Pre-bid meeting)

All enquiries from the bidder(s) relating to this Bid Document (if required) must be submitted to MRSAC by 06.02.2025 till 05:30 PM. These queries should also be emailed to [adm-mrsac@mrsac.gov.in](mailto:adm-mrsac@mrsac.gov.in). The queries should necessarily be submitted in the following format as a XLS & PDF Document:

*Table 4 Queries format*

SN	Bid Document Reference (Volume, Section No., Page No.)	Content of the Bid Document requiring clarification	Clarification Sought / Query
1			
2			
3			
...			

Queries submitted post deadline mentioned in this tender document, or which do not adhere to the above-mentioned format may not be responded to. All the responses to the queries (clarifications/corrigendum) shall be made available at <https://mahatenders.gov.in/>

## 6.8 Amendments to Bid Document

At any time before the deadline for submission of bids, the Department may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder(s), modify the tender document by an amendment. All the amendments made in the document would be issued as a corrigendum to the tender document and shall be made available at <https://mahatenders.gov.in/>

The bidder(s) are advised to visit the website mentioned above on regular basis for checking necessary updates. Department also reserves the right to amend the dates mentioned in this tender document for bid process.

In order, to afford prospective bidder(s) reasonable time to take the amendment into account in preparing their bids, Department may, at its discretion, extend the last date for the receipt of Bids.

## 6.9 Rights to Terminate the Process

Department may terminate the Bid Document process at any time and without assigning any reason. Department makes no commitments, express or implied, that this process will result in a business transaction with anyone.

This Bid Document does not constitute an offer by Department. The bidder(s) participation in this process may result in Department selecting the bidder(s) to engage in further discussions and negotiations toward selection. The commencement of such negotiations does not, however, signify a commitment by Department to execute a contract or to continue negotiations. Department may terminate negotiations at any time without assigning any reason.

## 6.10 Language of Bids

The Bids prepared by the bidder(s) and all correspondence and documents relating to the bids exchanged by the bidder(s) and Department, shall be written in English language, provided that any printed literature furnished by the bidder(s) in another language shall be accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall govern.

If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the bidder(s).

## 6.11 Bid Submission Format

The entire proposal shall be strictly as per the format specified in this Bid Document. Bidder(s) shall ensure that the bid documents are submitted in the respective folder online at <https://mahatenders.gov.in/>

## 6.12 Online Bid Submission

- i. Complete bidding process will be online (e-tendering) in two folder system.
- ii. Proposals must be direct, concise, complete and must be submitted online only.
- iii. Bidder(s) shall furnish the required information on their technical and commercial proposals in the enclosed format only. In case of any deviations in the format, bid will be liable for rejection.
- iv. Bidder(s) should submit information & scanned copies in only PDF format in Pre-Qualification/Technical Folder as mentioned in the Bid Document.
- v. Uploaded documents of successful bidder(s) may be verified with the original before issuance of Purchase Order. The successful bidder(s) has to provide the originals to the concerned authority (if requested).
- vi. Only the soft copies of Pre-qualification, Technical & Commercial bids need to be uploaded on e-tendering website.
- vii. Also, the hard copy of the entire tender document uploaded online along with the attachments (excluding price bid) should be submitted to MRSAC within three (03) working days after online submission of the tender.
- viii. All documents to meet the Pre-qualification are mandatory, however, Department reserves right to waive minor non-conformity (which do not constitute material deviation) or call for clarifications/additional documents. The bidder(s) will have to submit additional document/clarification within 2 working days from the date of issue of the letter/mail seeking clarification/additional document.
- ix. The Department reserves the right to accept or reject any or all the tenders without assigning any reason.
- x. The following points need to be considered while submitting the bids:
  - a. Bidder(s) Tool Kit link (detailed Help documents, designed for bidder(s)) has been provided on e-Tendering website (<https://mahatenders.gov.in/>) in order to guide them through different steps involved during e-Tendering such as online procedure for tender document purchase, bid preparation, bid submission.
  - b. If any assistance is required regarding e-Tendering (registration/upload/download), please contact



e-Tendering Help Desk. MRSAC will not be responsible for any issues arises during responding of answers demand on <https://mahatenders.gov.in/>

- c. The tender notice/Tender document and clarifications/corrigendum (if any) shall be uploaded on e- Tendering website (<https://mahatenders.gov.in/>).
- d. The date and time for online submission shall be communicated on the e-tendering website <https://mahatenders.gov.in/>. The tenderers should ensure that their tender is prepared and submitted online before the expiry of the scheduled date and time. No delay on account of any cause will be entertained. Offers not submitted online will be rejected.
- e. In the event of the specified date for the submission of bids being declared a holiday, the bids can be submitted online up to the appointed time on the next working day for which MRSAC will make necessary provisions.
- f. MRSAC may, at its own discretion, extend the date for submission of bids. In such a case, all rights, and obligations of MRSAC and the bidder(s) shall be applicable to the extended time frame.
- g. The offers submitted as documents, by telex/telegram/fax/Email or any manner other than specified in point 'iv' of this section, will not be considered. No correspondence will be entertained on this matter unless requested by MRSAC.
- h. Printed terms and conditions of the bidder(s) will not be considered as forming part of their bid.

### 6.13 Procedure for Submission of Bids

- i. To view-Tender Notice, Detailed Time Schedule for this Tender, kindly visit following e-Tendering website: <https://mahatenders.gov.in/>
- ii. The bidder(s) participating first time for e-Tenders on <https://mahatenders.gov.in/> will have to complete the Online Registration Process for the e-Tendering portal.
- iii. All bidder(s) interested in participating in the online e-Tendering process are required to obtain Class III Digital Certificates. The tender should be prepared & submitted online using individual's digital signature certificate.
- iv. The interested bidder(s) will have to submit the amount of INR 15000/- online only, as tender fee (Non-refundable) for this tender before online Bid Submission stage of the tender schedule.

### 6.14 Two Envelope Bid System

Complete bidding process will be online (e-Tendering) in two bid system. The bidder(s) shall submit the bid proposal in two folders:

- i. Pre-Qualification & Technical Folder
- ii. Commercial Proposal

### 6.15 Supporting Documents for Bid

The following table is provided as the guideline for submitting various important documents along with the bid.

*Table 5 Supporting Documents for Bid*

SN	Type of Folder	Documents to be submitted
01	Pre- Qualification / Technical Folder	<ul style="list-style-type: none"> <li>✓ Bid Cover Letter</li> <li>✓ Power of attorney/board resolution to the authorized Signatory of the Bid</li> <li>✓ Scanned copy of Online payment receipt of E.M.D. or Bid Security of INR 50,00,000/- and Tender Fee of INR 15,000/-</li> <li>✓ Particulars of the bidder(s) (in the given formats)</li> <li>✓ Proof of Office address in Maharashtra</li> <li>✓ Copy of Certificate of Incorporation/Registration Certificate</li> <li>✓ Letter of authorization to attend bid opening</li> <li>✓ Copy of the audited balance sheet of the company and Certificate from the Chartered Accountant clearly stating the net worth &amp; Profit and Loss statement</li> <li>✓ Self-declaration letter for not being blacklisted by Central/State Govt. as per given format</li> <li>✓ Copy of valid Goods &amp; Service Tax Registration in India &amp; Copy of PAN Card</li> <li>✓ Copy of Work Order or Purchase Order</li> <li>✓ Project Completion certificate from client and/or Go-live certificate from client, wherever applicable</li> <li>✓ All other supporting documents as per Pre-qualification/Technical Qualification Criteria</li> <li>✓ Manufacturer Authorization Form [as per given format]</li> <li>✓ Self-declared Security Certificate (specifying no security related threats or non-compliances back doors, malware, virus etc.) pertaining to the supplied products</li> <li>✓ Technical Proposal</li> <li>✓ Non-Disclosure Agreement (NDA)</li> </ul>
02	Commercial Proposal Folder	<ul style="list-style-type: none"> <li>✓ Commercial Proposal Cover Letter</li> <li>✓ Commercial Bid (as per given format)</li> </ul>

**Note:**

1. Bidder(s) shall furnish the required information on their Pre-Qualification, technical and financial proposals in enclosed formats only.
2. Any deviations in format may make the tender liable for rejection.
3. Disclosure of Commercial information of the bid in Pre-Qualification/Technical Folder may be sufficient grounds for rejection of the bid.

**6.16 Earnest Money Deposit (EMD) and Refund**

Bidder(s) are required to submit EMD in the form of online of INR 50 Lakhs or in the bid security form valid for 180 days from the date of opening of bid. Bid shall be treated as invalid if scanned copies are not submitted online along with the bid. Bids shall be rejected if EMD in the online or bid security form is not received. No interest shall be payable on EMD till the completion of bid process within the stipulated time.

Unsuccessful bidder's bid security will be discharged/returned within 30 days after the issuance of award of contract. Due to unavoidable reasons if bid security deposit is not discharged or returned to unsuccessful bidder(s) within 30 days, then bidder(s) will not be liable to claim any interest on the extended period.

The successful bidder's bid security will be discharged upon the bidder accepting the Purchase Order (issued by department) and furnishing the performance security in the form of performance bank guarantee. The bid security of 5% of contract value may be forfeited if a bidder withdraws its bid during the period of bid validity or in case of a successful bidder, if the bidder fails:

- i. To accept the Purchase Order (issued by department) in accordance with the terms and conditions
- ii. To furnish performance bank guarantee as specified in the terms and conditions

### **6.17 Evaluation Process**

The evaluation process of the Bid Document proposed to be adopted by Department is indicated under this clause. However, Department reserves the right to modify the evaluation process at any time during the Tender process, without assigning any reason, whatsoever, and without any requirement of intimating the bidder(s) of any such change. Department shall appoint an Evaluation Committee (EC) to scrutinize and evaluate the technical and commercial bids received. The EC will examine the Bids to determine whether they are complete, responsive and whether the Bid format confirms to the Bid Document requirements. Department may waive any non- conformity in a Bid which doesnot constitute a material deviation according to Department.

The evaluation will be a 3-stage process:

- i. Pre-qualification evaluation of all bidders
- ii. Technical Evaluation of bidder(s) who qualified pre-qualification stage
- iii. Commercial Evaluation of bidder(s) who qualified technical evaluation stage

There should be no mention of bid prices in any part of the Bid other than the Commercial Bids.

### **6.18 Opening of Bid**

All the Bids received within the deadline shall be opened at MRSAC on the specified date and time mentioned in this tender document. The bidder(s) authorized representatives may present themselves if willing to and shall sign the attendance sheet. Once the bids are opened, each bid will be checked for pre-qualification criteria.

### **6.19 Evaluation of Technical Bids**

The Technical Bids of only those bidder(s), who qualify in the Pre-Qualification stage, shall be considered. For all responsive bids, the Evaluation Committee (EC) will invite each qualified bidder(s) to make a technical presentation as part of the technical evaluation.

The EC may require verbal/written clarifications from the bidder(s) to clarify ambiguities and uncertainties arising out of the evaluation of the Bid documents. Bidder(s) is expected to provide an executive summary in tabular format with clearly indicating their compliance with technical evaluation criteria along with index to the supporting documentary evidence in the proposal. The proposal must include all the documents specified in the section "Supporting Documents for Bid"

The bidder(s) are required to fill up technical specification Compliance Table, as per Annexures. Non-Compliance, if any, should be brought out very clearly. If bidder(s) fails to submit the Compliance Tables, giving any false information, in response to information sought in this RFP, their offer shall be rejected

Following will be the technical evaluation methodology:

- i. Each Technical Bid will be assigned a technical score out of a maximum of 100 marks.
- ii. Bidder(s), who attain total technical score of 70 (seventy) or more, will qualify for the evaluation of commercial bids.
- iii. The commercial bids of bidder(s) who do not qualify technically shall not be opened.
- iv. The committee shall indicate to all the bidder(s) the results of the technical evaluation through online. The technical scores of the bidder(s) will be announced prior to the opening of the commercial bids.

v. Table 6 Evaluation Criteria

Sr. No.	Evaluation Criteria	Basis of Evaluation	Max Marks	Supporting Document
<b>1</b>	<b>SI's Commercial &amp; Professional Strength</b>		<b>15</b>	
1.1	Cumulative annual turnover of SI for the last three audited financial years FY 2021-22, 2022-23 and 2023-24) from IT/ITES services.	<p>≥Rs.50Cr.and&lt; 60 Cr: 7 marks</p> <p>≥Rs.60Cr.and&lt; 70 Cr: 8.5 marks</p> <p>≥Rs.70Cr.: 10 marks</p>	10	<p>Audited Balance sheets and Profit &amp; Loss account statements of the SI for each of the last three audited financial years FY 2021-22, FY 2022-23, FY 2023-24</p> <p>AND</p> <p>CA certificate clearly stating the turnover from IT/ITES Services</p>
1.2	<p>Certification:</p> <p>The SI should possess the following valid certification as on bid submission date</p> <p>ISO 9001, 20000, 27001 and CMMI Level 5</p>	<p>ISO 9001 &amp; ISO 20000: 3.5 marks</p> <p>ISO 9001, ISO 20000 &amp; ISO 27001: 4 marks</p> <p>ISO 9001, ISO 20000, ISO 27001 and CMMI Level 5 (All Four) – 5 marks</p>	5	<p>Copy of valid certificate of, ISO 9001, 20000, 27001 issued by the competent authority and CMMI Level 5</p>
<b>2</b>	<b>Experience and competence of the SI</b>		<b>25</b>	
2.1	<p>Number of Projects involving infrastructure implementation in on-premises IT hardware and software setup in India completed/undertaken (in India) of similar nature and value as specified in next column. The work order should have been issued within the last 7 years, as on bid submission deadline of this RFP.</p> <p>Weightages (W) In case project is completed (i.e., Go-live and 100% of Maintenance Period): 100% weightage. In case project is in</p>	<p>Number of projects where SI have implemented or have been maintaining infrastructure -</p> <p>a. 3 No of Project of INR 6 crore – 7 marks</p> <p>b. 2 No of Project of INR 9 crore – 8.5 marks</p> <p>c. Single Project of INR 17 crore and above – 10 marks</p>	10	<p>Work order (WO)/Contract document(s) and Completion certificate(s) from client and Project Citation in the attached format.</p> <p>OR</p> <p>Work order WO)/Contract document(s) and Go-live certificate(s) from client and Project Citation (including completion % of Maintenance period) in the attached format.</p> <p>All above supporting documents shall mandatorily mention the value of project and duration of the contract.</p>

	progress, Go- live has been completed and >=50% of maintenance period is completed: 80% weightage. In case project is in progress, Go-live has been completed and <50% of maintenance period is completed: 60% weightage.			
2.3	Project experience: on-premises infrastructure Setup projects completed/undertaken (in India) of similar nature and value as specified in next column. The work order should have been issued within the last 7 years as on bid submission deadline of this RFP.	SI should have been maintaining on premise Infrastructure Setup projects: 1(one) project: 11 marks 2 (two) projects: 13 marks 3 (three) projects: 15 marks	15	Copy of Letter of Award (LOA)/Purchase Order (PO)/Work Order /Contract Agreement along with valid certificates.
<b>3</b>	<b>Proposed Project Resources</b>		<b>25</b>	
3.1	Project Manager/Team Leader (1 position)	Qualification: B. Tech / BE / MCA or equivalent along with Relevant Certification (PMP, Prince2, Agile etc.): No. of years of relevant experience: For >8 years to 12 years: 7 marks For >12 years: 10 marks	10	Provide the roles against which the CVs have been provided by the SI as per the format provided in Form-10 of this RFP duly signed by the Authorized Signatory of the SI along with the copy of the
3.2	Systems Engineer (1 positions)	Qualification: B. Tech / BE / MCA /BCA /BSc IT or equivalent with Relevant certification in Operating Systems (MCSE / MCSD / MCSA) or equivalent and No. of years of relevant experience: > 4 yrs.: 4 marks For additional year of relevant experience >6yrs: 1 mark	5	Provide the roles against which the CVs have been provided by the SI as per the format provided in Form-10 of this RFP duly signed by the Authorized Signatory of the SI along with the copy of the Certification, if applicable

3.3	Network Engineer (1 positions)	Qualification: B. Tech/BE/MCA /BCA /BSc IT or equivalent and Relevant Certification (CCNP/CCNA/ACE-A/JNCIA/ADCNS/ASTA/ACSS or equivalent) and No. of years of relevant experience: >4 yrs: 4 marks For additional year of relevant experience >6yrs: 1 mark	5	Provide the roles against which the CVs have been provided by the SI as per the format provided in Form-10 of this RFP duly signed by the Authorized Signatory of the SI along with the copy of the Certification, if applicable
3.4	Cyber Security Engineer (1 positions)	B. Tech / BE / MCA /BCA /BSc IT or Equivalent and Cyber Security certification No. of years of relevant experience: > 4 yrs: 4 marks > 6yrs: 1 mark	5	Provide the roles against which the CVs have been provided by the SI as per the format provided in Form-10 of this RFP duly signed by the Authorized Signatory of the SI along with the copy of the Certification, if applicable
4	<b>Technical Presentation</b>		<b>35</b>	
		Understanding of SOW: 7 marks Competence/Capability of SI: 7 marks Strategy for O &M phase: 7 marks Focus, clarity, coherence of the presentation: 7 marks Project Management Methodology for Implementation Phase: 7 Marks  to Evaluation Committee.  The SI shall submit copy of the presentation delivered to the committee.	35	Presentation to the evaluation committee.

		<p>Total (Tb) Marks will be awarded as per the following criteria:</p> <p>Poor: 1 mark</p> <p>Average: 2 marks</p> <p>Good: 3 marks</p> <p>Very Good: 4 marks</p> <p>Excellent/Outstanding: 5 marks</p>		
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--



## 6.20 Guidelines for composition of Technical Proposal

- i. The technical response must meet all the mandatory compliance requirements. For complete details on the undertakings and formats, as mentioned in this RFP.
- ii. The technical proposal shall address all the areas/sections as specified by the RFP and should contain a detailed description of how the bidder(s) will provide the required services outlined in this RFP. It should articulate in detail, as to how the bidder(s) Technical Proposal meets the requirements specified in this RFP. The technical proposal must not contain any pricing information. If the technical proposal contains any commercial information, the proposer is liable to be rejected. In submitting additional information, please mark it as “supplementary” to the required response. If the bidder(s) wishes to propose additional services (or enhanced levels of services) beyond the scope of this RFP, the proposal must include a description of such services as a separate and distinct attachment to the proposal.
- iii. The technical proposal must furnish details about previous project experience for the criterion in the technical evaluation matrix in the format provided in the RFP.
- iv. Technical proposal must have a compliance sheet for requirement specifications as given in this RFP.
- v. The Technical Proposal should be structured under the following minimum heads, failing which bid shall be rejected:
  - a. Overview of the proposed IT infrastructure that meets the requirements specified in the RFP
  - b. Overall proposed technology, and deployment architecture
  - c. Security architecture
  - d. Integration and Interfacing Architecture
  - e. Network architecture
  - f. Bill of material of all the components (i.e., software, hardware, etc.) as per the formats provided in the RFP
  - g. Approach & methodology for project development, management and implementation including the project plan
  - h. Project team structure, size, capability, and deployment plan (Total Staffing plan including numbers)
  - i. Training and Communication Strategy for key stakeholders of the project
  - j. Project Management, reporting and review methodology
  - k. Strategy for conducting Operations & Maintenance
  - l. Risk Management approach and plan
  - m. MAF from the OEMs on the software and hardware proposed by bidder(s)
  - n. Bidder(s) experience in all the project related areas as highlighted in Bid evaluation criteria
  - o. Bidder(s) must provide the team structure and the resumes of key profiles within each team in the format provided in the RFP.

- p. Bidder(s) must ensure that all profiles shared should be unique and separation of duties is ensured.
- q. Comprehensive Project Plan along with manpower deployment plan and resources to be dedicated to the project.
- r. The technical proposal shall also contain bidder(s) plan to address the key challenges anticipated during the execution of the project.
- s. The proposed infrastructure shall meet all the minimum specifications mentioned in this RFP. The bidder(s) shall provide compliance matrix for each of the proposed components indicating compliance.
- t. The bidder(s) should give details of all the proposed IT and Non-IT components, without specifying the costs in the format given below:

SN	Name of Item	OEM/Make	Exact Model	Quantity/License Count Offered
1	Item 1			
2	Item 2			
...				

Make and Model (one & only one unique Make and Model per BOQ item is required) of all proposed components along with datasheets highlighting Technical Specification parameters in each datasheet for compliances.

#### **6.21 Period of Validity of Bids**

Bids shall remain valid for the period of 180 days after the bid submission deadline date prescribed by Department. A bid valid for a shorter period shall be rejected by Department as non-responsive.

In exceptional circumstances, prior to the expiration of the bid validity period, Department may request bidder(s) to extend the period of validity of their Bids. The request and the responses shall be made in writing. In this case, the EMD shall also be extended for thirty (30) days beyond the deadline of the extended validity period. A bidder(s) may refuse the request without forfeiting its EMD. A bidder(s) granting the request shall not be required or permitted to modify its bid.

No interest will be paid by Department on amount of EMD.

#### **6.22 Clarification of Bids**

To assist in the examination, evaluation, and comparison of the Bids, and qualification of the bidder(s), Department may, at its discretion, ask any bidder(s) for a clarification of its bid. Any clarification submitted by a bidder(s) that is not in response to a request by Department shall not be considered, and Department's request for clarification and the response shall be in writing. If the Bid includes a financial proposal, no change in the prices or substance of the bid shall be sought, offered, or permitted, except to confirm the correction of arithmetic errors discovered by Department in the evaluation of the Bids.

If bidder(s) does not provide clarifications of its bid by the date and time set in Department's request for clarification, its bid shall be rejected.

Clarification(s) will be sought through email only ([admin-mrsac@mrsac.gov.in](mailto:admin-mrsac@mrsac.gov.in)) and the response to the clarification shall be received email only

### **6.23 Non-Material Non-Conformities**

Provided that a bid is substantially responsive, Department may waive any non-conformity in the bid that does not constitute a material deviation, reservation, or omission.

Department may request that the bidder(s) to submit the necessary information or documentation, within a reasonable period, to rectify non-material non-conformities in the bid related to documentation requirements. Requesting information or documentation on such non-conformities shall not be related to any aspect of the price of the bid. Failure of the bidder(s) to comply with the request may result in the rejection of its bid.

Department may rectify non-material non-conformities related to the Bid Price. To this effect, the Bid Price shall be adjusted, for comparison purposes only, to reflect the price of a missing or non-conforming item or component.

### **6.24 Opening of Commercial Bid**

The commercial bids of only technically successful bidder(s) will be opened on mentioned web portal only.

The Commercial Bids will be opened and assessed by Department for completeness and accuracy. Bidder(s) are advised to fill the Excel file (as per the format provided) very carefully.

Please note:

- If there is a discrepancy between the prices (for Schedules A, B & C) mentioned in the Excel file and PDF file, price mentioned in the Excel file shall prevail.
- If there is a discrepancy between words and figures, the amount in word shall prevail unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to the points above.

Activities and items described in the Technical Proposal but not priced, shall be assumed to be included in the prices of other activities or items. In case an activity or line item is quantified in the Financial Proposal differently from the Technical Proposal, the Evaluation Committee may correct the quantification indicated in the Financial Proposal so as to make it consistent with that indicated in the Technical Proposal, apply the relevant unit price included in the Financial Proposal to the corrected quantity to arrive at total value to be considered for commercial evaluation.

If the bidder(s) does not accept the correction of errors, its bid will be rejected, and the bid security may be forfeited.

Bidder(s), while quoting against this tender, must take cognizance of all concessions permissible, if any, under the statutes and ensure the same is passed on to the Department failing which it will have to bear extra cost. In case bidder(s) does not avail concessional rates of levies like GST, customs duty, excise duty, sales tax, etc. Department will not take responsibility towards this.

The bidder(s) shall fully familiarize themselves about the applicable domestic taxes (GST, service tax, income

taxes, duties, fees, levies, etc.) on amounts payable to the Department under the resultant Agreement. All such taxes must be included by bidder(s) in the financial proposal. Should there be a change in applicable taxes, the prevailing taxes on the date of billing would prevail.

## **6.25 Evaluation of Commercial Bids and Award Criteria**

The technically qualified bidder(s) will further be selected on Quality and Cost based Selection (QCBS) where marks will be given in 70:30 ratios (70 marks for Technical Evaluation and 30 Marks for Financial Evaluation). For evaluation of the bids, Quality and Cost based Selection (QCBS) method will be adopted as per the formula given below:

The scores will be calculated as:

$$Ob = [(0.7) \times (T_b / T_{max}) \times 100] + [(0.3) \times (C_{min} / C_b) \times 100]$$

Where

- i.  $Ob$  = Overall score of SIs under consideration (calculated up to two decimal points)
- ii.  $T_b$  = Technical score for the SI under consideration
- iii.  $T_{max}$  = Highest Technical score as per the technical proposals under consideration
- iv.  $C_b$  = Commercial price of the SI under consideration
- v.  $C_{min}$  = Lowest commercial as per the financial proposals under consideration

The bidder(s) achieving the highest overall score will be invited for negotiations for awarding the contract. In case of a tie where two or more bidders achieve the same highest overall score, the bidder with the higher technical score will be invited first for negotiations for awarding the contract. In case of a tie on the technical scores and highest overall scores, the  $C_b$  will be calculated to the third place of decimal and the bidder with lesser  $C_b$  will be invited for negotiations for awarding the contract. The work order will be awarded to the bidder who's overall score ( $Ob$ ) is highest.

## **6.26 Terms and Conditions**

All terms & conditions mentioned in each section of this tender document shall be valid throughout the term. All the commitments made by the bidder(s) through correspondences for the completion of the tender process shall be applicable throughout the term.

The conditions mentioned in Purchase Procedure Rules and Instructions as per Government of Maharashtra.

COMPLIANCE OF RESTRICTIONS FOR COUNTRIES WHICH SHARE LAND BORDER WITH INDIA Restrictions under Rule 144(xi) of the General Financial Rules, 2017 – Reference OM no. 6/18/2019 – PPD dtd. 23.07.2020 (read along with any subsequent clarifications/amendments thereof) issued by Ministry of Finance, Public Procurement Division (<https://doe.gov.in/procurement-policy-divisions>)

As per Government Resolution no. Bha.kha.sa-2014/ Pra. Kra. 82/Section-III/Industry-4 dated 1.12.2016 if the bidder(s) quotes the price below 20% or above 10% of the estimated price then the bid of the respective

bidder(s) will be rejected.

## **6.27 Rights to Accept/Reject any or all Proposals**

Department reserves the right to accept or reject any proposal, and to annul the bidding process and reject all Bids at any time prior to award of Contract, without thereby incurring any liability to the affected bidder(s) or any obligation to inform the affected bidder(s) of the grounds for Department's action.

## **6.28 Fraud and Corruption**

Department requires that bidder(s) must observe the highest standards of ethics during the execution of the contract. In pursuance of this policy, Department defines, for the purpose of this provision, the terms set forth as follows:

- i. "Corrupt practice" is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party.
  - ii. "Fraudulent practice" is any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation.
  - iii. "Collusive practice" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party.
  - iv. "Coercive practice" is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party.
  - v. "Obstructive practice" is
    - a. deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Department investigation into allegations of a corrupt, fraudulent, coercive, or collusive practice; and / or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation, or
    - b. Acts intended to materially impede the exercise of Departments in section and audit rights.
- Bidder(s) should note that:
1. If it is noticed that the bidder has indulged into the Corrupt/Fraudulent/Unfair/Coercive practices, it will be a sufficient ground for Department to terminate the contract and initiate blacklisting of the vendor.
  2. Department will reject a proposal for award if it determines that the bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract.
  3. Department will sanction a firm or individual, including declaring in eligible, either in definitely or for a stated period of time, to be awarded a department-financed contract if it at any time determines that the firm has, directly or through an agent, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for, or in executing, a department- financed contract; and
  4. Department will have the right to require that a provision be included in bidding documents and in contracts financed by Department, a provision be included requiring

bidder(s), suppliers, and contractors to permit Department to inspect their accounts and records and other documents relating to the bid submission and contract performance and to have them audited by auditors appointed by Department.

#### **6.29 Notifications of Award and Signing of Contract**

Prior to the expiration of the period of proposal validity, the bidder(s) will be notified in writing or by email that their proposal has been accepted.

The notification of award will constitute the formation of the Contract. Upon the bidder's executing the contract with Department, it will promptly notify each unsuccessful bidder(s) and return their EMDs.

At the time Department notifies the successful bidder that their bid has been accepted, Department will send the bidder the Performa for Contract, incorporating all clauses / agreements between the parties. Within 14 days of receipt of the letter of intent, the successful bidder must sign and date the Contract along with format of PBG and return it to Department.

#### **6.30 Performance Bank Guarantee**

The Selected bidder shall at his own expense, deposit with Department, within fourteen (14) working days from the date of issuance of the notification of award of the contract or prior to signing of the contract, whichever is earlier, an unconditional and irrevocable Performance Bank Guarantee (PBG) from any Scheduled or Nationalized bank as per the format given in this Bid Document, payable on demand, for the due performance and fulfillment of the contract by the bidder.

This Performance Bank Guarantee will be for an amount equivalent to 5% of purchase order value (including the value of GST) and shall be valid for 3 months after the completion of the Contract with the successful bidder. All charges whatsoever such as premium, commission, etc. with respect to the Performance Bank Guarantee shall be borne by the bidder. The Performance Bank Guarantee format is given in this document. The Performance Bank Guarantee may be discharged/returned by Department upon being satisfied that there has been of due performance of the obligations of the bidder under the contract. However, no interest shall be payable on the Performance Bank Guarantee.

In the event of the selected bidder being unable to serve the contract for whatever reason, Department would invoke the PBG. Not with standing and without prejudice to any rights whatsoever of Department under the Contract in the matter, the proceeds of the PBG shall be payable to Department as compensation for any loss resulting from the bidder's failure to complete its obligations under the Contract. Department shall notify the selected bidder in writing of the exercise of its right to receive such compensation within 14 days, indicating the contractual obligation(s) for which the bidder is in default.

Department shall also be entitled to make recoveries from the selected bidder's bills, performance bank guarantee, or from any other amount due to him, the equivalent value of any payment made to him due to inadvertence, error, collusion, mis construction or misstatement.

#### **6.31 Stamp Duty**

The successful bidder shall enter into a contract agreement with Department within 30 days from the date of issue of the notification of award and the same should be adjudicated for payment of Stamp Duty by the successful bidder. The contract agreement should be registered with IGR and all expenses including (but not

limited to) stamp duty, legal charges and incidental expenses in this respect shall be borne and paid by the successful bidder.

## **7 Scope of the Work:**

### **7.1 Introduction:**

Maharashtra Remote Sensing Application Centre (MRSAC) was established in September 1988 at Nagpur as an autonomous organization under the administrative control of department of planning, Govt. of Maharashtra. Today, MRSAC is one of the well-established Centre. With full support of Govt. of Maharashtra, MRSAC is recognized as a premier institution to offer benefits of Remote Sensing and Geographic Information System (GIS) technologies to the State. With its experience of more than three decades, MRSAC has promoted technology to Govt. departments and academic Institutions for various applications.

The Geo-spatial application areas which can be served by MRSAC, related to various departments, include soil and water conservation, watershed development and monitoring, Ground water prospect, Water supply and Sanitation, forest and biodiversity studies, Crop acreage Estimation, Coastal studies, urban development, Rural Development, Education as well as Public Health, etc. The Centre is making sincere efforts for perseverance of natural resources of the State by providing innovative and effective solutions to natural resources management challenges. MRSAC is striving hard to make effective use of Remote Sensing & GIS technologies for achieving twin targets of meeting the demands of increasing population and maintaining ecosystem balance by way of creating data warehouse and information dissemination.

MRSAC is also established in development of Web portals and mobile applications for various departments under GoM. MRSAC has team of software programmers which provide all the technical support and services regarding webportal development, mobile apps development with geotagging and geofencing capabilities, server installation, server maintenance, webportal migration, training the field officers, etc. Following is some of the departments and its Decision Support systems containing web portals and mobile apps:

- Agriculture

- MahaAgritech
- MahaMADAT (Drought)
- Warehouse Mapping

- Water Resources

- Jalyukt Shivar
- WSSD
- GSDA
- NHP-DSS
- WRD
- MTS
- GMD
- IWMP

- Relief &  
Rehabilitation

- E-Panchnama

- Forest
  - Vanyukt Shivar- (2cr / 4 cr / 13 cr / 33 cr / 2020 / 2023 Plantation)
  - MahaVAN – Integrated Mobile Apps
- Infrastructure
  - RIS
  - PMGSY
- Utilities
  - School Mapping
  - Health Mapping
  - RUSA
  - Sports Mapping
  - MEDA
  - Akola GIS
  - Ahmednagar GIS
- Urban
  - DMA (Hawker Street Vendor Mapping)
  - CIDCO
- Industrial
  - MIDC
  - MSME
- Ports
  - MPT
  - JNPT
  - MMB
- GatiShakti
  - MSEDCL Electric Pole Mapping
  - Traffic Pole Mapping
  - MSME Industries Mapping
- Others (MRSAC's Initiatives)
  - Rainfall Analysis
  - Covid-19 Surveillance
  - Smart Village
  - Explore
  - Osmanabad GIS
  - SAMMS



The Govt. of Maharashtra has declared MRSAC as the “State Nodal Agency” for procurement of satellite imageries on behalf of Government of Maharashtra and share it with user departments, after processing, through Maharashtra Geo-spatial Digital Database System–(MGDDS) under MahaBHUMI project. MRSAC is, also, entrusted with the role of custodian of Remote sensing and GIS information on central server and develop a decision support system for use of RS/GIS database in State.

In this connection, MRSAC intends to enhance the current IT Infrastructure on premise for creation of Image Base library using high resolution Satellite data & feature abstraction in various thematic maps, leading to creation of a Geo-Spatial Database. A GIS based decision support system for user departments is also envisaged in this project. Accordingly, MRSAC will be generating voluminous data (Peta bytes) in the next 5 (five) years. In order to meet this requirement, the capacity of IT infrastructure for MahaBHUMI needs to be upgraded appropriately and shall include (but not limit to) latest IT hardware/software since the current environment cannot meet the requirements of the above-mentioned initiatives. Currently, the production, development, staging and maintenance environment of these GIS applications are hosted On Prem. MRSAC intends to host the production GIS applications on Cloud through another RFP while retaining the development, staging and maintenance environment On Premise. MRSAC intends to select the System Integrator (SI) who shall upgrade, operate, and maintain the existing MRSAC on premise infrastructure at Nagpur for a period of five (05) years for hosting their development, staging and maintenance environment. The detailed scope of the work (SOW) is as below.

The bidder shall perform the following activities as per the scope of work given below:

- i. Supply, Installation, Testing, Commissioning, Operations & Maintenance of IT Infrastructure for setting up of development, staging and maintenance Environment at MRSAC, Nagpur.
- ii. Setup a state-of-the-art robust security architecture that provides end-to-end security solution for the entire IT infrastructure and applications. The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, etc. The bidder must make provisions for security of all hardware as well as protection of the software system from hackers and other threats that include the following items.
  - Cyber-attacks/Denial of Service (DoS and DDoS) attacks from the Internet.
  - Hacking into the data repositories from the Internet.
  - Injection of malicious software from the Internet.
  - Sniffing of data and MITM attacks.
  - Ransomware protection
  - User identity impersonation and credentials stealing.
  - Insider Threat: To prevent insider, threat the solution should have identity & access management, audit trail and Log management
  - Using Firewalls and Intrusion Prevention Systems, afore mentioned threats should be prevented and well supported (and implemented) with the security policy.
- iii. Through another RFP, MRSAC is planning to onboard an MSP/CSP for migration of existing MRSAC applications from the current On-premises data center hosted at Nagpur to a cloud. System Integrator shall support MSP/CSP and MRSAC during the migration of such applications from the current on-premises hosted at MRSAC Nagpur to the proposed Cloud DC or DR.

- iv. Bidder should also provide support for integrating the on-premises application and the applications hosted on the cloud as and when required in consultation with MRSAC.
- v. Bidder should also provide the tickets raised in manual form till the ticketing tool is been deployed in the IT infrastructure.
- vi. Bidder should also be responsible for the connectivity between Cloud and On-Premises IT infrastructure at MRSAC Nagpur, in coordination with on-boarded CSP/MSP and in consultation with MRSAC.

The System Integrator's scope of work shall include but will not be limited to the following broad areas. Details of each of these broad areas of activity have also been outlined in subsequent sections of this document:

#### Design Principles

- i. End-to-End No Single point of failure architecture.
- ii. Scalability - Technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of MRSAC. The system should also support horizontal scalability (maximum 25% of existing hardware and software) so that depending on changing requirements from time to time, the system may be scaled upwards.
- iii. Flexibility - System should provide easily configurable interfaces for integration with any future application/system (internal or external to MRSAC). System should be capable enough to handle structured, unstructured data and should be platform agnostic.
- iv. Availability - Components of the architecture must provide redundancy and ensure that there are no single point of failures in the key project components.
- v. Manageability - Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and therefore should be catered for in proposed solution.

#### **Existing Infrastructure:**

The existing on-premises infrastructure hosted at MRSAC Office, Nagpur is currently used by MRSAC users (Scientist and GIS experts) to develop and maintain the GIS platform for the state of Maharashtra.

Currently, the production, development, staging and maintenance environment of these GIS applications are hosted On Prem. MRSAC intends to host the production GIS applications on Cloud through another RFP while retaining the development, staging and maintenance environment On Premise.

Considering the criticality of the data intensive GIS applications, which will form the base for various digital initiatives in Maharashtra, it is crucial to retain the on-Premises infrastructure for development, staging and maintenance environment upto date and secure.

Currently at MRSAC, there are 14 physical Blade servers and Network Storage System (NAS) of 800 TB and unified Storage of 20 TB and smaller NAS 32 TB and 64 TB, Core switch of 48 SFP+ ports of 10Gbps speed and 05 nos. of access switch of 1Gbps speed and other unmanaged switches. MRSAC have some local tower physical servers for antivirus, license servers such as ESRI, Hexagon, AutoCAD, Tally etc., 200 workstations and desktops and 14 quantities of HIPS.

## **7.2 Supply, Installation, Commissioning, Operations & Maintenance of IT Infrastructure:**

## List of Hardware and Software Components:

The list of new hardware and software items as per RFP is enlisted below and its detail specifications are provided in Technical Specification (refer Section 7.3).

*Table 7 List of Hardware and Software Components*

Sr. No.	Component	Quantity
<b>Hardware Components</b>		
1.	Router	2
2.	Link Load Balancer with DDOS	2
3.	Server Load Balancer with WAF	2
4.	Network Firewall	4
5.	Switch Type - I	2
6.	Switch Type - II	10
7.	Switch Type - III	2
8.	Hyper Converged Infrastructure (HCI)	1
9.	Server Type - I	8
10.	SAN switches	2
11.	NVMe SSD Storage (100 TB)	1
12.	Unified Storage System (1 PB)	1
13.	Backup Storage system with Backup software (1.2PB)	1
14.	RACK with KVM & Console	6
15.	LED Monitor: Size 59 cm with compatible adapter, cables, and wall mount kit with matrix switch	4
<b>Software Components</b>		
1.	HIPS (40 applications)	1 Lot
2.	Endpoint detection and response (EDR)	1 Lot
3.	NMS (upto 400 devices) perpetual license	1
4.	Asset Monitoring Software, Asset Management, Patch Management (upto 400 devices) perpetual license	1
5.	Operating System-Windows server 2022 or latest 64 bit	100
6.	Virtualization Software	16

- i. The above-mentioned common data center services shall be provisioned by the System Integrator/Bidder at MRSAC premises.
- ii. The list and the sizing provided are only indicative and not exhaustive. Bidder(s) may analyze the requirements based on the understanding and propose the required infrastructure and sizing with proper justification to meet MRSAC's requirements.

## 7.3 Detailed Technical Specifications

### 7.3.1 Router

Sr. No.	Specifications of Router	Compliance (Yes / No)
1.	The Router should be purpose-built device with 2U / 4U	
2.	Router should have Minimum 4-Ports of 1 Gbps of Ethernet Base-T port and 4 ports of 10 Gbps SFP+ MM port	
3.	The Router should provide minimum aggregate throughput bandwidth of 30 Gbps.	
4.	The Router should support minimum 10 million packets.	
5.	The Router should have minimum 4 GB RAM.	
6.	The Router should support out of band management access via USB/Console/Auxiliary port	
7.	The Router should support IPsec tunneling for site-to-site VPN to the remote sites.	
8.	The Router should support IPv4 and IPv6, IPv4/IPv6 Dual Stack, Static routes, OSPF, RIPv2, BGP, IS-IS, Policy-Based Routing (PBR) or ECMP for Traffic Management.	
9.	The Router should support classless inter domain routing (CIDR) IP default gateway.	
10.	The Router should support Multicast Internet Group Management Protocol (IGMPv2/V3).	
11.	The Router should support RADIUS, SNMP Notification Logging, NetFlow/JFlow or Equivalent	
12.	The router should not have any single point of failure, like power supply and fans, the Router should operate on 230v and should have redundant power supply	

### 7.3.2 Linked Load Balancer (LLB) and Distributed Denial of Service (DDoS)

Sr. No.	Technical Requirement Specification (Minimum)	Compliance (Yes/No)
1.	The proposed solution should be purpose build-based hardware appliance with dual power supply. The appliance must not allow or support to deploy Open Source/3rd party Network Functions on the same appliance as virtual instance.	
2.	The Web Application Firewall shall have at least 04 nos. 10G base-X ports populating 10Gig SR complying to IEEE 802.3ae standard and The Web Application Firewall shall have minimum 04 nos. 1x Gig ports from day 01.10gig interface should be upgradeable to 25Gig by changing transceivers only.	
3.	Proposed solution should have 1 x RJ45 console and dedicated out-of-band management port.	
4.	The solution should have at least 32 GB of memory to ensure there is no performance degradation, with a minimum of 450GB of SSD storage for storing logs.	
5.	Should support minimum 15 Gbps of L7 throughput from day 1.	
6.	The proposed appliance must provide minimum SSL TPS of 14K with RSA 2K keys and 8K TPS with ECC ECDSA P-256 from day 1 and Minimum 10 Gbps hardware based SSL throughput (bulk encryption)	
7.	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active in both DC & DR	

	Environments. The solution must support N+1 architecture to provision more than 2 appliances in a HA cluster to achieve horizontal scaling	
8.	The solution shall be provided in High Availability in Active-Active and Active-Passive Mode configuration, when deployed in dual mode and should have seamless takeover in-case if one device fails. It should also support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check.	
9.	The Proposed hardware must have Dual power supply with hot swappable feature	
10.	Proposed solution should have Anti DDOS, DNS Security; Link Load Balancer, Global Server Load balancer, DNSSEC feature, Authoritative DNS, Recursive DNS and DNS DDOS functionalities. The solution must not be part of any UTM or NGFW or any white labeled or virtual solution SK running on third party hardware. The bidder is free to provide these technologies on a single or multiple appliances.	
Link Load Balancer (LLB)		
11.	System should support both in.-bound & out-bound load balancing.	
12.	System should support termination of at least 4 internet/intranet links to load balance and ensures the active- active and active-standby capabilities on link traffic.	
13.	The document/cross reference provided by the OEM for each clause asked in the RFP must be available on a GLOBAL public domain and the proposed solution must support all technical features specified in the RFP from day 1. OEM Simple undertaking without any test results/proofs claiming any performance number will not be accepted.	
14.	The software solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the software solution across cloud environments and integration with automation and CI/CD tools including Ansible, Jenkins, and Terraform. The solution shall support overlay network like VxLAN/Geneve for integration with kubernetes services	
15.	System should support multi path health monitoring along with the capability to create complex health checks using Log expressions to monitor the link status.	
16.	Should be intelligent to handle multiple link of different capacity and able to utilize the same accordingly. System should support dynamically redirecting traffic via the best performing link.	
17.	The proposed solution must provide below application optimization features: 1) TCP Optimization: Should be able to modify TCP parameters like keep alive interval, maximum RTO, window size, Nagle Algorithm, delay window control, packet loss ignore rate, flow control, congestion control speed etc. on the fly to improve application performance 2) Compression: Solution should be able to provide cost-effective offloading of traffic compression processing to improve page load times and reduce bandwidth utilization. 3) Caching: Solution should be able to do caching to reduce network traffic and increase application performance	
18.	The proposed appliance must be able to load balance both TCP and UDP traffic from L3 to L7. The proposed solution must have the capability to provide SSL offloading using both RSA and ECC based keys	

19.	System should support setting a priority for each type of traffic.	
20.	Should support Geolocation and Proximity based load balancing	
21.	Solution should support traffic shaping/Bandwidth Management from Day 1.	
22.	Offered product should be IPv6 Ready	
23.	Should support Static NAT, PAT & Dynamic NAT.	
24.	Shall provide individual health check for each link.	
25.	Should have predefined health checks on protocols like TCP, UDP & ICMP	
26.	The offered solution should provide full Authoritative DNS capability to understand records like A, AAAA, CNAME, DNAME, HINFO, MX, NAPTR, NS, PTR, SOA, SRV, TXT	
27.	Supports an GUI integrated zone file management tool that simplifies DNS zone file management and reduce the risk of misconfiguration. It shall provide a secure environment to manage DNS infrastructure while validating and error-checking zone files. It shall be built on the latest version of BIND.	
28.	Deliver high speed standard (non-GSLB) DNS query responses. E.g. addressing queries at very high speed by obtaining configuration via zone transfer from primary authoritative DNS Servers and accommodate large numbers of zones and records	
29.	Solution should enable IT administrators to set up DNS security extensions (DNSSEC) to validate signing keys and ensure connected DNS servers are the right ones	
30.	Should support the following Global Load balancing algorithms. <ul style="list-style-type: none"> <li>• Round robin</li> <li>• Global availability</li> <li>• Application availability</li> <li>• Geography</li> <li>• Least connections</li> <li>• Packets per second</li> <li>• Round trip time</li> <li>• Packet completion rate</li> <li>• Dynamic ratio</li> <li>• LDNS</li> <li>• Ratio</li> </ul>	
31.	Should be able to do on the fly DNSSec - Can the product convert DNS requests to DNSSec on the fly	
32.	Should support 1) Delegated DNS and 2) Proxy DNS	
33.	Should be able to define amount of memory for use of DNS caching and specific portions of the cache can be discarded without restarting the server	
34.	GSLB Persistency: GSLB should support persistency based on TTL, CIDR (IPv4 and IPv6) Should have persistence synchronization between GSLB devices	
35.	Support DNS SEC validation by acting as a recursive name server to verifies all of the signatures from the answer back to the closest trust anchor (a public key it knows and trusts)	
36.	Should have DNS64 functionality, without scripting	
37.	The proposed solution should have the capability to dynamic connection reaping feature to close idle TCP connections.	

38.	The proposed solution should have the capability to define the below TCP parameters at a global level and granularly per application level: a. TCP Close Wait b. TCP FIN Wait c. TCP Idle Timeout d. TCP Keep Alive Interval	
Distributed Denial-of-Service (DDoS)		
39.	Should protect ICMP attacks: ICMP floods, ping floods, smurf, IP Spoofing, LAND attack, Teardrop, IP Option Timestamp, IP Option Route Record, IP Option Source Route, Ping of Death, Tracert, ICMP Redirect, ICMP Unreachable, ICMP Large Packet.	
40.	The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL handshake attack	
41.	The proposed hardware must support TLS 1.3 Perfect Forward Secrecy Support	
42.	Should protect TCP based attacks: TCP SYN Flood, TCP SYN- ACK Flood, TCP ACK Flood, TCP FIN/RST Flood, TCP Connection Flood, TCP Slow Connection, TCP Abnormal Connection, TCP Fragments Flood, Defence WinNuke & TCP Error Flag	
43.	The solution should provide the traffic AUTO learning function for the DDOS traffic monitoring and should be capable of creating signature in real time (to be backed by publicly available document)	
44.	System should be able to support multiple segment protection.	
45.	System Should detect and mitigate IPv6 and IPv4 Attacks.	
46.	System should provide protection for volumetric and Protocol level DDoS attacks.	
47.	Inspection and prevention are to be done in same hardware.	
48.	The proposed solution should have a mitigation mechanism to protect against zero-day DoS and behavioural DoS attacks without manual intervention and be able to create auto signatures for zero-day DDoS attacks and DNS DDOS attacks.	
49.	The DDOS solution must be resilient enough to mitigate following types of attacks: DNS reflection, DNS Amplification, Floods attacks like TCP, UDP, ICMP, IGMP, ARP, Bad header floods, SMURF attack, tear drop attack, DNS caching poisoning, protocol anomalies based attacks, DNS Tunneling attack, DNS based exploits.	
50.	DDOS should prevent signature based and TPS based attacks at Network, DNS and SIP level	
51.	The proposed solution should have at least 100 DOS Vectors in-built.	
52.	The solution should provide the multi-level DDOS mitigation policy and different mitigation action based on DDOS traffic type.	
53.	The solution should Access control list for IP, TCP, UDP, DNS, URL, blacklist and whitelist	
54.	The solution should support Access control list based on inbuilt GeoIP with configurable duration.	
55.	The proposed solution must support protocol inspection	
56.	Proposed DDOS solution should detect any DDoS traffic and mitigate any DDOS attack without interrupting any legitimate traffic and customer services.	
Monitoring, Reporting and Management		

57.	The system must support configuration via standard up to date web browsers. System user interface must be based on HTML.	
58.	Role/user-based access control should be available	
59.	The solution must be able to generate summary attack report of daily/weekly/monthly	
60.	Should support SNMP v2 & v3 traps, email alerts and SNTP/ NTP. Device should be able to send SNMP traps to centralized server and should provide login/ logout, configuration changes, dumps information.	
61.	The LLB & DDoS Solution shall support SNTP/NTP for date & time synchronization from the NTP server.	
62.	The LLB & DDoS Solution shall be manageable (both GUI and CLI) using telnet, SSH, Web based management (HTTPS), etc.	
63.	The LLB & DDoS Solution shall have a feature to provide role-based access	
64.	Should support authentication, authorization and accounting (AAA) integration with external authentication support providers such as RADIUS and TACACS+ and support RBAC to help ensure security. Should support role-based access.	
65.	Should Support integration with SIEM and other Monitoring and AG Reporting solution	
66.	Proposed LLB & DDoS solution must be of same OEM as of hardware vendor and not a 3rd party solution integrated with hardware and supplied.	
67.	The proposed LLB & DDoS solution should have online diagnostic tool, where administrator can take snapshot of configuration to diagnose the DDoS vulnerability and the OS related issue on the fly and tool should provide the recommended or necessary steps to patch those DDoS vulnerabilities	
68.	The solution shall support the provisioning of the reports - Attack reports -top sources, targets, attack type, Attack Severity Distribution, Attack Source Region	
69.	The solution must support the generation of pdf reports containing the detailed statistics and graphs and It should have capability to send those reports through email.	
70.	Proposed solution's operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions	
71.	Management solution should have the capability to store the logs for more than 90 days.	
72.	Quoted solution should be deployed in India in at least 3 Data Centre / Govt. customer reference in India and should provide evidence of the same	
73.	The OEM should have a Technical Assistance Center (TAC)with India Toll Free Numbers	
74.	The OEM should have Support Centers/Service Center or 24x7x365 TAC Support.	
75.	Solution can be a combination of both LLB and DDoS in a single appliance or multiple appliances from same OEM. If the bidder is providing DDOS as separate appliance, then the DDOS appliance must support throughput of 15 Gbps.	

### 7.3.3 Server Load Balancer (SLB) with WAF



Sr. No	Technical Requirement Specification (Minimum)	Compliance (Yes/No)
Hardware Details each SLB and WAF Device		
1.	Proposed hardware platform should be of high performance, highly scalable, and purpose-built next Generation platform for application security and Web Application Firewall (WAF) from same OEM running on same OEM OS version and platform; Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware.	
2.	The document/cross reference provided by the OEM for each clause asked in the RFP must be available on global public domain like product datasheets, product guides etc. and the proposed solution must support all technical features specified in the RFP from the date of issue of this RFP	
3.	Bidder/OEM may be asked to demonstrate all the technical features asked in the RFP through a POC and any non-compliance in the technical functionality/feature will lead to rejection of the bid.	
4.	The Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber. The hardware of all these ports should be complete in all respect. 10gig interface should be upgradeable to 25Gig by changing transceivers only.	
5.	The Web Application Firewall shall have minimum 04 nos. 1x Gig ports from day 01	
6.	The Web Application Firewall shall have a 100/1000 Base Tx Port for out of bound management.	
7.	The Web Application Firewall shall have a console port based on RS-232 / RJ-45 for configuration and diagnostic AS purposes.	
8.	The Web Application Firewall shall have enough CPU capacity and 64GB Memory so as to efficiently meet all the capability parameters as well as functionalities laid down in the specifications.	
9.	The Web Application Firewall hardware shall be designed to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.	
10.	The Web Application Firewall shall be capable of working with AC Power supply with a Voltage varying from 170 -240 Volts at 50 +/- 2 Hz.	
11.	The Web Application Firewall shall have internal Redundant Power Supply (RPS). The primary as well as redundant power supply shall be hot swappable, and no downtime/reboot shall be required for addition/removal of power supply module.	
12.	The Web Application Firewall shall support 19" Rack mounting with 1U form factor.	
Solution Capabilities		
1.	The Solution shall have minimum 15 Gbps L4-L7 throughput.	
2.	The Web Application Firewall Solution shall have minimum 35 million concurrent TCP connections.	
3.	The Web Application Firewall Solution shall have minimum 03 Lakh L4 TCP connections/second.	
4.	The Web Application Firewall Solution shall have minimum 1 million HTTP request/second.	

5.	The WAF shall support minimum 28,000 RSA and 14,000 ECC SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse.	
6.	The Application Delivery Controller shall support minimum of 15 Gbps SSL throughput and compression of 15 Gbps.	
7.	The Web Application Firewall Solution shall support HTTP1.0, HTTP1.1 & HTTP/2 protocols.	
8.	The software solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the software solution across cloud environments and integration with automation and CI/CD tools including Ansible, Jenkins, and Terraform.	
Support for Native and Kubernetes integration Features with license upgrade		
1.	The Web Application Firewall shall support integration with REDHAT OpenShift Kubernetes Platforms and requisite controller/license/container plugin shall be provided with WAF solution from day one. Controller/Plug-in should be from same make as WAF. It should not be third party or opensource.	
2.	The Controller/Container Plugin shall support both Nodeport and ClusterIP mode of deployment and also as an Ingress service.	
3.	The Controller/Container Plugin shall support Application Delivery Controller orchestration to dynamically create and manage WAF objects.	
4.	The Controller/Container Plugin shall support PER NAMESPACE operations with the capability to run Ingress service plugins on a PER NAMESPACE basis	
5.	The Web Application Firewall shall be support to forward traffic to container cluster via NodePort and ClusterIP.	
6.	The Controller/Container Plugin shall support the configuration of advanced services like Web application firewalls through declarative syntax.	
7.	The Controller/Container Plugin shall support integration using latest Container network interface (CNI) for the container platform.	
8.	The Web Application Firewall shall support NodePort mechanism for integration with kubernetes services.	
9.	The Web Application Firewall shall support BGP for integration with kubernetes services.	
10.	The Web Application Firewall shall support overlay network like VxLAN/Geneve for integration with kubernetes services	
11.	WAF should integrates with REDHAT Openshift container orchestration environments to dynamically create L4/L7 services on WAF, and load balance network traffic across the services. Monitoring the orchstration API server, Solution should be able to modify the WAF configuration based on changes made to containerized applications.	
12.	Installation of Controller/Container Plugin should be using Operators on OpenShift Cluster and Helm charts.	
13.	Controller/Container Plugin should support use of open shift route resources and support route annotations.	
14.	Controller/Container Plugin should use multiple Virtual IP addresses	
15.	Controller/Container Plugin should use Custom resources extensions of the Kubernetes API. It should registers to the Kubernetes client-go using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update,	

	and delete events. Resources identified from such events are pushed to a Resource Queue maintained by controller.	
Web Application Firewall Solution Functional Requirements		
	The Web Application Firewall shall support the following Mode of deployment:	
1.	Reverse proxy deployment Cluster deployment Inline bridge deployment The Web Application Firewall Solution shall support the following Load Balancing Features Support for 200 servers	
2.	Support load balancing algorithms Least connection Ratio Round Robin weighted Least connection	
3.	The Web Application Firewall Solution shall support both a positive security model and a negative security model. A negative security model explicitly defines known attack signatures. The negative security model shall include a pre-configured comprehensive and accurate list of attack signatures and Web application firewall shall allow specific signatures to be modified by the administrator.	
4.	The Web Application Firewall Solution shall be able to learn the Web Application Structure & elements to address the difficulty of configuring the positive security model.	
5.	The Web Application Firewall Solution in learning mode shall be able to recognize application changes while simultaneously protecting Web applications and learned values shall be used as the configuration for input checking in the positive security model.	
6.	The Web Application Firewall Solution shall support custom security rules. Administrators shall be able to define rules for the positive or negative security models. The WAF should support specific profiling like parameter length, meta characters etc. sk to configure granular controls for specific deployed web application.	
7.	The Web Application Firewall Solution shall support the following Action Mode: Block Block & Report Report only	
8.	The Web Application Firewall Solution shall support full coverage of OWASP Top 10 web application security risks: A1-Injection A2-Broken Authentication A3-Sensitive Data Exposure A4-XML External Entities (XXE) A5- Broken Access Control A6-Security Misconfiguration A7- Cross-Site Scripting XSS A8-Insecure Deserialization AG A9-Using Components with Known Vulnerabilities	

	A10-Insufficient Logging & Monitoring	
9.	<p>The Web Application Firewall Solution shall prevent the Following attacks:</p> <ul style="list-style-type: none"> <li>XSS</li> <li>SQL injection</li> <li>Directory\path traversal</li> <li>Forceful browsing</li> <li>HTTP response splitting</li> <li>OS command injection</li> <li>LDAP injection</li> <li>SSI injections</li> <li>XPath injection</li> <li>Sensitive information leakage (e.g., CCN, SSN, custom defined)</li> <li>Application DOS / DDOS</li> <li>CSRF</li> <li>Evasion and illegal encoding</li> <li>XML validation</li> <li>Web services method restrictions and validation</li> <li>HTTP RFC violations</li> <li>Form field tampering</li> <li>Parameter tampering</li> <li>Form field manipulation</li> <li>Session hijacking</li> <li>Protocol validation</li> <li>XML and Web services protection</li> <li>Web application vulnerabilities</li> <li>Cookie poisoning</li> <li>Application buffer overflow</li> <li>Brute force</li> <li>Access to predictable resource locations</li> <li>Unauthorized navigation</li> <li>Web server reconnaissance</li> <li>HTTP request format and limitation violations (size, unknown method, etc.)</li> <li>Use of revoked or expired client certificate</li> <li>File upload violations</li> </ul>	
10.	The Web Application Firewall Solution shall support Zero-day attacks prevention.	
11.	The Web Application Firewall Solution shall be able to prevent automated layer 7 DDoS attacks, web scraping, and brute force attacks from being directed to the site.	
12.	The Web Application Firewall Solution shall have "anti-automation" protection which can block the automated attacks using hacking tools, scripts, frameworks, etc.	
13.	The Web Application Firewall Solution shall support the attack expert system provides an immediate, detailed description of the attack, as well as enhanced visibility into the mitigation techniques used to detect and prevent the attack.	
14.	The Web Application Firewall Solution shall support Web scraping using javascript with support for white list of scrappers for allowable scraping.	

15.	The Web Application Firewall Solution must be able to protect Web Scraping by configuring customized rules/scripts e.g. rules to detect & drop a POST request to a specific URL that does not have a cookie inserted by web application firewall.	
16.	The Web Application Firewall Solution shall support AJAX/JSON application security for interactive web2.0 based applications.	
17.	The Web Application Firewall Solution shall have an Integrated XML firewall to provide application-specific XML filtering and validation functions that ensure that the XML input of web-based applications is properly structured. It provides schema validation, common attacks mitigation, and XML parser denial-of-service prevention.	
18.	The Web Application Firewall Solution shall support server cloaking which hides error pages and application error information.	
19.	The Web Application Firewall Solution shall support integration with VA scanning tools to imports the XML report and provide a quick fix of the vulnerabilities including Acunetix, Qualys, Rapid 7, IBM Appscan etc. to virtually patch web application vulnerabilities.	
20.	The Web Application Firewall Solution shall provide Data leak prevention by Identifying and blocking sensitive information transmissions such as credit card numbers (CCN) and social security numbers (SSN).	
21.	The Web Application Firewall Solution shall fully address PCI DSS 2.0 Requirement	
22.	The Web Application Firewall Solution shall have PCI compliance report.	
23.	The Web Application Firewall Solution shall have the option to pass selective file extension.	
24.	The Web Application Firewall Solution shall have the option to block selective file extension.	
25.	The Web Application Firewall Solution shall have a dynamic blacklist for temporary blocking of Attack Source.	
26.	The Web Application Firewall Solution shall be able to define separate security policies (including attacks to be blocked, inspections to be applied, etc, working mode (i.e., report mode only or blocking mode)) for different HTTP/HTTPS host (FQDN) or URLs.	
27.	The Web Application Firewall Solution shall have Advance security features with:	
	The proposed solution should have server stress based L7 Behavioural DOS detection and mitigation including the ability to create real time L7 DOS signatures.	
	The proposed solution should provide behavioral DoS (BADoS) which provides automatic protection against DDoS attacks by analyzing traffic behavior using machine learning and data analysis.	
	The proposed solution must support Single Sign-On functionality on the same appliance running on the same OS version from the same OEM in the future. The solution must protect against FTP, SMTP, HTTP, HTTPS, and Application layer Dos and DDOS attacks including stress based DOS and Heavy URL attacks.	
	The proposed solution should have the capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating JavaScript and CAPTCHA challenges.	
	The proposed WAF should support of prevention of theft as well as the mitigation of attacks that uses previously stolen credentials.	

	The proposed WAF solution should protect from automated attacks on Web and mobile apps, and against bots that emulate human behavior	
28.	The Web Application Firewall Solution shall support switching the security modules from learning/passive to active/blocking mode.	
29.	The Web Application Firewall Solution shall support automatic updates to the signature database, ensuring complete protection against the latest application threats.	
30.	The Web Application Firewall Solution shall have the Geo-location based IPv4 & IPv6 database. So, Geo-location based traffic filtering shall be done on the Web Application Firewall.	
31.	Solution defend the applications against automated attacks and bots through Anti-bot Protection and categories bot in to category like:- Browser, trusted bot, untrusted bot, Suspicious Browser, Malicious Bot, Unknown etc.	
32.	The Web Application Firewall Solution shall have static routing capabilities for IPv4 & IPv6.	
33.	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions/shortcuts to address the compliances and configure policies for it.	
34.	The WAF solution must support Security Policy to be applied per application, rather than one single policy for an entire system.	
35.	System should support inbuilt ability or integration with any 3rd party solution to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be generated for audit and compliance.	
36.	The administrators should be able to see all the signatures and not just the signature categories. Admins can apply Specific signatures to specific policies	
37.	WAF should provide ability to enforce a given user to follow a sequences of pages while accessing	
38.	should have GraphQL protection that automatically detects and mitigates GraphQL related attacks on both GraphQL and JSON formats.	
Management & Reporting		
1.	The Web Application Firewall Solution shall support Syslog, SNMP (v2c & v3) & MIB-II.	
2.	The Web Application Firewall Solution shall support NTP / NTP for date & time synchronization from the NTP server.	
3.	The Web Application Firewall Solution shall be manageable (both GUI and CLI) using telnet, SSH, Web based management (HTTP, HTTPS), etc.	
4.	The solution should provide online troubleshooting and traffic analysis tool where the administrator can take a snapshot of the config and upload it on web based diagnostic tool to check the health and vulnerability of the solution with the recommended solution provided on the knowledge base link.	
5.	WAF should provide the application visibility and reporting with the below metrics and entity for each application: • Client IP addresses/subnets as well as geographical regions	

	<ul style="list-style-type: none"> <li>• Total Transactions as well as Average and Max Transactions/sec</li> <li>• Most commonly requested URLs</li> <li>• Server Latency and Page Load times</li> <li>• Virtual Server and Pool server performance</li> <li>• Page Load Time</li> <li>• Response code</li> <li>• OS and Browser</li> <li>• URL details</li> </ul>	
6.	The Web Application Firewall Solution shall have a feature to provide role based access	
User's access for management		
1.	The Web Application Firewall Solution & Management & Reporting Solution shall support authentication & authorization through Radius / TACACS+.	
2.	The Web Application Firewall Solution shall support upload /download of device configuration through secure communication with Management Server.	
3.	The management server must support the archiving and it shall be able to export logs/events using NFS/SMB/SCP/SFTP.	
4.	The Web Application Firewall Solution shall support integration with SIEM. The Web Application Firewall Solution shall be able to send logs to SIEM Servers.	
5.	Security events should be exportable via SNMP, SMTP, Syslog and other industry standard formats to meet auditing and regulatory compliance requirements	
6.	The Web Application Firewall shall generate alarms w.r.t. health status of Server/s, security alarms for TCP SYN attacks, DoS attacks, etc.	
7.	<p>The Web Application Firewall shall provide comprehensive reports (both realtime as well as Historical for at least 03 months) that can be customized as per requirement. Following are a few examples of the reports:</p> <p>Client side concurrent TCP connections per virtual server/application/URL.</p> <p>Client side new TCP connections per second per virtual server/application/URL.</p> <p>Server side concurrent TCP connections per server.</p> <p>Server side new TCP connections per second per server.</p> <p>Total Input as well as Output "Bytes per second" OR "Bits per second" per vserver/application/URL in order to have the usage of Internet Bandwidth.</p> <p>Total Input as well as Output "Bytes per second" OR "Bits per second" between the equipment and a particular Server.</p> <p>Server Uptime and downtime reports.</p> <p>CPU and Memory utilization of the equipment.</p> <p>Dozens of predefined Web application security reports such as session hijacking, non-valid XML structure, CCN leakage</p> <p>Reports detailing learned application resources</p> <p>Audit and access reports</p> <p>PCI compliance reports allow to drill down to relevant PCI DSS section providing system compliance information</p> <p>Top attackers, Top targeted applications, Top Intrusions/Attacks</p> <p>Reports based on Anonymous Proxies, TOR IP addresses &amp; Malicious IP addresses.</p>	
8.	The Historical Reports shall be provided for multiple timeframes i.e., hourly, daily, weekly, monthly, and customized periods.	

Regulatory Compliance of each WAF device		
1.	The Web Application Firewall shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standards like IS-13252 (Part 1):2010 for Safety requirements of Information Technology Equipment.	
2.	The Web Application Firewall shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standards like IS 6873(Part 7):2012 for EMC (Electro Magnetic Compatibility) requirements.	
Product/OEM Evaluation Criteria		
1.	WAF/WAF's Operating System should be tested and certified for EAL 2/NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, MeitY, Govt. of India.	
2.	The WAF solution should be in the Gartner's, Kpingercole, IDC, SecureIQ Magic Quadrant of Latest published Report Web Application and API Protection/WAF.	
High Availability		
1.	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active	
2.	Should support transparent failover between 2 devices, the failover should be transparent to other networking devices with SSL session mirroring.	
3.	Should support network-based failover for session mirroring, connection mirroring and heartbeat check	
4.	Device level HA should support automatic and manual synchronization of configuration from the primary device to the secondary device.	

#### 7.3.4 Network Firewall

Sr. No.	Specifications of Next Generation Firewall	Compliance (Yes / No)
1.	The Firewall should be Hardware based, purpose-built security appliance with hardened operating system and should be an application-aware device.	
2.	The Firewall should support IP Security VPN technologies, Secure Sockets Layer (IPsec/SSL) VPN technologies.	
3.	The Firewall must be provided with minimum 10 Gbps of Firewall and threat prevention throughput of minimum 9 Gbps after enabling IPS, Application control and Advanced Malware Protection.	
4.	The Firewall should support a DES/AES VPN Throughput of at least 50 Gbps	
5.	Firewall should support at least 5,000 concurrent VPN peers both IPsec & SSL. 200 SSL VPN / remote tunnels should be provisioned with the solution.	
6.	The Firewall should support VPN clustering, VPN load-balancing.	
7.	The Firewall should support min 4 million Concurrent Connections	
8.	The Firewall should support min 5 lakh new Connections/Second	
9.	The Firewall should have 8 x-1Gb Ethernet ports, 8x1Gb SFP Slots & 8x10 Gbps ports or SFP MMFibre ports.	
10.	The Firewall should support Integrated Network Ports	



11.	The Firewall should support 802.1q VLAN interfaces, 250 Virtual Interfaces (VLANs) and should support logically separate firewalls. Ten (10) Virtual zones Firewalls/logical systems should be provisioned.	
12.	The Firewall should support Active/Active, Active/Standby High Availability feature	
13.	The Firewall should support USB 2.0 Ports, RJ-45 (console)	
14.	The Firewall should have min of 16 GB of system Memory	
15.	Should be provided with OEM supplied Rack Mount Kit for mounting in 19" Rack.	
16.	Firewall must support IPS functionality on TCP traffic with all IPS signatures enabled.	
17.	IPS application must support centralized event correlation and reporting mechanism.	
18.	IPS must support the following detection mechanisms: exploit signatures, protocol anomalies and application controls	
19.	IPS and firewall module must be integrated on one platform.	
20.	The Firewall should support L2 and L3 (Routed) mode.	
21.	The Firewall must support IPv4 and IPv6 features.	
22.	The Firewall should support dynamic, static and policy-based NAT / PAT services.	
23.	The Firewall should support HTTP, HTTPS, or FTP Filtering.	
24.	The Firewall should support deep inspection services for Web traffic for improved protection from a wide range of Web-based attacks	
25.	The Firewall should support IPv6-enabled inspection services for HTTP, FTP, SMTP, ICMP, TCP, UDP	
26.	DoS detection - Protection against SYN flood, IP, ICMP, and application attacks.	
27.	The Firewall should support DES, 3DES, AES-128, 256 encryption standards and support IPsec VPN solution.	
28.	Extensive monitoring, troubleshooting and debugging from CLI should be supported.	
29.	The Firewall should support real time monitoring through external syslog servers	
30.	The Firewall should Simple Network Management Protocol (SNMP) and should be accessible through console port, Telnet, SSSHv1, SSHv2	
Firewall Management		
31.	The Security Management solution be implemented in a dedicated server/hardware with 4TB storage, 4core CPU and 16GB memory and should have licenses for all software components required for Logging, Reporting Event correlation etc.	
32.	The Firewall should a graphical Device Manager, command line interface (CLI) and syslog.	
33.	The Firewall should support real time Log & event monitoring with exhaustive Event correlation and reporting capabilities. All components required to give one dashboard view of security should be provided from day one.	
34.	The firewall log should be seamlessly integrated with the SIEM solution.	

### 7.3.5 Network Switch (Type-I)

Sr. No.	Specifications of Core Switch	Compliance (Yes / No)
1.	Switch shall be provided with 16 ports of 10 Gbps and 16x40 Gbps QSFP	
2.	The Switch must be provided with fully populated with all the required SFPs.	
3.	The switch should support non-blocking Layer 2 switching and Layer 3 routing.	
4.	The switch should not have any single point of failure like power supplies and fans etc. should have 1+1 / N+1 level of redundancy	
5.	Switch should provide switching capacity of 3.6 Tbps	
6.	The switch should support 200K MAC address.	
7.	Switch Should have port forwarding rate of minimum 1.2 bpps.	
8.	Switch should support the complete STACK of IP V4 and IP V6 services.	
9.	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied.	
10.	Switch should have console, management port	
11.	Switch should have adequate power supply with all slots populated N+1 redundant	
12.	Switch should support VLAN tagging (802.1q), IEEE Link Aggregation and Ethernet Bonding	
13.	Switch should support Configuration roll-back and check point, support for different logical interface types like loop back, VLAN, SVI, Port Channel, multi chassis port channel / LAG etc.	
14.	The switch should support IPv4 and IPv6 routes entries in the routing table including multicast routes	
15.	Switch should support Graceful Restart for OSPFv2, OSPFv3, IS-IS, BGP etc. and should support static and dynamic routing using OSPF V.2, IS-IS using, BGP, PIM-SM PIM-SSM for IP V4 and IP V6 protocols	
16.	Switch should support services such as IP routing (static / dynamic), IP Forwarding, Policy based Routing, ACL, QoS.	
Layer2 Features		
17.	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S), VLAN Trunking (802.1q) and should support minimum 4000 VLAN, Multicast IGMP v2, v3	
18.	Support for broadcast, multicast, and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and Vulnerabilities	
19.	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
Layer3 Features		
20.	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and should support layer 3 VLAN Interface and Loop back port Interface	
21.	Support RFC 3618 Multicast Source Discovery Protocol (MSDP), IGMP V.2 and V.3	
22.	Switch should support for deploying different security for each logical and physical interface using access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail	
23.	Switch should support processor/CPU and memory Protection from unnecessary or DoS traffic by security protection policy.	

24.	Switch should support for role-based access control for restricting host level network access as per policy defined	
25.	Configuration through the CLI, Console, Telnet, and SSH SNMPv1, v2, and v3 and Remote monitoring (RMON) support NetFlow/JFlow or equivalent for traffic analysis, should support tools like Ping and Traceroute, Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port, RADIUS/TACACS+ or equivalent for switch security access administration, Network Time Protocol (NTP) or equivalent support	
26.	Switch should support for QoS in IPv4/IP V.6 network connectivity	
27.	Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as: SNMPv1, SNMPv2c, SNMPv3	
28.	All licenses should be provided with the devices for the mentioned features. The licenses should be perpetual in nature.	

### 7.3.6 Network Switch (Type-II)

Sr. No.	Specifications of Managed Access Switch	Compliance (Yes / No)
1.	The switch should have 24 nos. 10 Gbps Ethernet Base-T MM, 4 X 25Gbps SFP28Uplinks fully populated with required transceivers	
2.	Shall have minimum 680 Gbps of switching capacity	
3.	Switch Should have port forwarding rate of minimum 800 Mpps.	
4.	The switch should support 100K MAC address.	
5.	The switch must support Stacking/MLAG or equivalent configuration and to be configured for high availability with necessary cable / modules to be supplied with the switch	
6.	The switch should have stacking/MLAG or equivalent support minimum 4 switches in a single stack/PoD with stacking/MLAG	
7.	Switch shall support to create PoDs of multiple switches using industry standard technologies like MLAG or equivalent	
8.	The switch should support an Internal redundant Power Supply and fans	
9.	The switch should support IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p, IEEE 802.1Q Trunking, IEEE 802.1s Multiple Spanning Tree (MSTP), IEEE 802.1w Rapid Spanning Tree (RSTP), IEEE 802.1x, IEEE 802.1AB Link Layer Discovery Protocol (LLDP), IEEE 802.3ad Link Aggregation Control Protocol (LACP), IEEE 802.3x full duplex, IEEE 802.1Q VLAN encapsulation, IEEE 802.1x	
10.	The switch should support RMON standards, SNMP v1, v2c, and v3, Spanning-tree, IGMP filtering, Multicast Listener Discovery (MLD)/IGMP, LLDP, UDLD / Bridge assurance / BFD, LACP, ARP, DHCP or IGMP snooping.	
11.	The switch should support discovery of the neighbouring device giving the details about the platform / IP Address / Link connected through etc.	
12.	Static Routing for IPv4 and IPv6	
13.	Shall support Strict Priority Queuing (SP) / Weighted Fair Queuing (WFQ) / Weighted Deficit Round Robin (WDRR)configurable buffers and Explicit Congestion Notification (ECN)	

14.	The switch should support Control- and Data-plane QoS ACLs	
15.	Shall support ACL or port ACL or IPv4/IPv6 ACL	
16.	Shall support applying QoS policies on a port, VLAN, or whole switch, to set priority level or rate limit selected traffic	
17.	The switch should support Command Line Interface (CLI) support for configuration & troubleshooting purposes.	
18.	The switch should support four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis	
19.	The switch should support Trivial File Transfer Protocol (TFTP) /SCP/SFTP to reduce the cost of administering software upgrades by downloading from a centralized location	
20.	The switch should support SNMP v1, v2c, and v3 of-band management.	
21.	The switch should support Telnet interface, support for comprehensive in- band management of band management.	
22.	The switch should support Port-based ACLs or ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.	
23.	The switch should support SSHv2 and SNMPv3 to provide network security.	
24.	The switch should support TACACS+ / RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.	
25.	The switch should support RFC 951 - Bootstrap Protocol (BOOTP) or DHCP	
26.	The switch should support VLAN, MAC address / ARP / route notification to allow administrators to be notified of users added to or removed from the network.	
27.	The switch should support Port security to secure the access to an access or trunk port based on MAC address.	
28.	The switch should support Multilevel security on console access to prevent unauthorized users from altering the switch configuration.	
29.	The switch should support DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addresses DHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.	
30.	The switch should support DHCP Interface Tracker feature to augment a host IP address request with the switch port ID.	

### 7.3.7 Network Switch (Type-III) – HCI Switch

Sr. No.	Specifications of Core Switch	Compliance (Yes / No)
1.	Switch shall be provided with 24 port (25 Gbps SFP28) MM and uplink 4x40 Gbps QSFP/4X100 Gbps QSFP	
2.	The Switch must be provided with fully populated with all the required SFPs.	
3.	The switch should support non-blocking Layer 2 switching and Layer 3 routing.	
4.	The switch should not have any single point of failure like power supplies and fans etc. should have 1+1/N+1 level of redundancy	
5.	Switch should provide switching capacity of 3.6 Tbps	
6.	The switch should support 200K MAC address.	

7.	Switch Should have port forwarding rate of minimum 1 bpps.	
8.	Switch should support the complete STACK of IP V4 and IP V6 services.	
9.	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied.	
10.	Switch should have console, management port	
11.	Switch should have adequate power supply with all slots populated N+1 redundant	
12.	Switch should support VLAN tagging (802.1q), IEEE Link Aggregation and Ethernet Bonding	
13.	Switch should support Configuration roll-back and check point, support for different logical interface types like loop back, VLAN, SVI, Port Channel, multi chassis port channel / LAG etc.	
14.	The switch should support IPv4 and IPv6 routes entries in the routing table including multicast routes	
15.	Switch should support Graceful Restart for OSPFv2 , OSPFv3, IS-IS, BGP etc. and should support static and dynamic routing using OSPF V.2, IS-IS using, BGP, PIM-SM PIM-SSM for IP V4 and IP V6 protocols	
16.	Switch should support services such as IP routing (static /dynamic), IP Forwarding, Policy based Routing, ACL, QoS.	
Layer2 Features		
17.	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S), VLAN Trunking (802.1q) and should support minimum 4000 VLAN, Multicast IGMP v2, v3	
18.	Support for broadcast, multicast, and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
19.	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
Layer3 Features		
20.	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and should support layer 3 VLAN Interface and Loop back port Interface	
21.	Support RFC 3618 Multicast Source Discovery Protocol (MSDP), IGMP V.2 and V.3	
22.	Switch should support for deploying different security for each logical and physical interface using access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail	
23.	Switch should support processor / CPU and memory Protection from unnecessary or DoS traffic by security protection policy.	
24.	Switch should support for role-based access control for restricting host level network access as per policy defined	
25.	1.) Configuration through the CLI, Console, Telnet, and SSH SNMPv1, v2, and v3 and Remote monitoring (RMON). 2.) Support NetFlow / JFlow or equivalent for traffic analysis. 3.) Should support tools like Ping and Traceroute. 4.) Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port.	

	5.) RADIUS / TACACS+ or equivalent for switch security access administration, Network Time Protocol (NTP) or equivalent support	
26.	Switch should support for QoS in IPv4/IP V.6 network connectivity	
27.	Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as: SNMPv1, SNMPv2c, SNMPv3	
28.	All licenses should be provided with the devices for the mentioned features. The licenses should be perpetual in nature.	

### 7.3.8 Hyper Converged Infrastructure Solution (HCI)

Sr. No.	Specifications of Hyper Converged Infrastructure (HCI)	Compliance (Yes / No)
1.	The Hyper Converged Infrastructure (HCI) system must be provided as an integrated appliance solution pre-installed with server nodes, virtualization hypervisor, network, Software Defined Storage (SDS), data protection, high availability, and comprehensive management	
2.	The HCI solution should deliver enterprise class storage services using latest x86 servers without dependence on a separate Storage Area Network or SAN switches or HBAs	
3.	The HCI solution must support scaling of storage capacity and performance linearly by addition of nodes	
Nodes and cluster		
4.	The HCI must have an initial configuration of 12 nodes (10 regular nodes and 2 GPU nodes)	
5.	Each node must have the following or better configuration: Rack server with rack mount kit.	
	CPU: 2 x Intel Xeon Gold 3rd Generation/AMD EPYC 32-core processor with base frequency of 2.8 GHz or higher.	
	RAM: 768 GB DDR4 3200 MHz using 64 GB modules or higher. Network: 4x25 GbE SPF28, 1x1 GbE for Management.	
	Redundant hot swap power supplies and cooling fans of suitable capacity Required separate boot device.	
6.	All nodes must be enterprise class x86 servers from one of the major enterprises reputed and leading OEMs	
7.	The solution must tolerate at least one node failure	
8.	The HCI must be scalable to 32 nodes or higher in a single cluster	
9.	Must have online cluster grow & shrink capability	
10.	The two GPU nodes must each be populated with 1 No Ampere A100 40 GB PCIe GPU card along with vCompute Server/necessary required software licenses	
11.	The GPU nodes must be supplied with full capacity redundant power supplies and cooling fan 1s as appropriate for the GPU configuration	
12.	The GPU server nodes and the entire HCI solution including hypervisor, SDS and management software must be fully compatible and certified for the enterprise GPUs and Softwares.	

13.	Necessary licenses for GPU virtualization should be supplied by the vendor to use the supplied GPU cards	
Storage		
14.	The HCI storage solution must be scale out Software Defined Storage (SDS) distributed across the nodes. It must pool disk drives from all nodes to present single storage resource pool to all server nodes	
15.	Must have thin provisioning of storage	
16.	The HCI solution should be configured for (300 TB) with 100 TB SSD and 200 TB SAS	
17.	NL-SAS for Cluster 1 & 2 storage capacity or higher must be provided across all nodes. The usable capacity must be net usable storage space excluding cache capacity and after RF=2 or equivalent implementation.	
Virtualization, Hypervisor		
18.	Enterprise server virtualization features must be built into the HCI solution	
19.	Must be compatible with all standard guest OSs (in particular: Windows Server 2012, Windows Server 2016, Windows 10, Windows 8, RHEL, CentOS, Ubuntu)	
20.	Virtualization software must have the capability to create virtual machine templates to provision new servers	
21.	Must provide minimal downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure	
22.	Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS.	
23.	Must enable configuration of virtual machines for 1 node or 2 nodes failure	
24.	Must have virtual machine High Availability	
25.	Must provide intelligent virtual machine placement and initial VM placement in a cluster and distribution of VMs across nodes in a cluster.	
26.	Virtualization software should provide network traffic-management controls to allow flexible allocation of physical NIC between different network- traffic types and allow user-defined network/bandwidth, Enabling multi- tenancy deployment and should support 802.1Q for multi vlan traffic.	
27.	Must provide live migration of running virtual machines from one node to another with zero downtime and continuous service availability	
28.	In the event of node failure, virtual machines should automatically move and run on other designated node(s)	
29.	Hypervisor should provide the ability to hot add CPU, memory, disks and NICs on the fly without any service/VM disruption.	
30.	Must have virtual machine automated resource scheduling and auto load balancing of resources across nodes and VMs	
31.	Must provide virtual machine affinity rules	
32.	Must provide for creation and restore of snapshots for individual virtual machines.	
33.	Must allow taking clones of individual virtual machines and have an integrated wizard for batch clones of virtual machines and customization	
34.	Must support Layer 2 virtual switches with VLAN support	
35.	Should have firewall to manage virtual port of VMs	

36.	Should support HA for migration of VMs in case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software. Should support HA for VMs with a passthrough PCIe device or a NVIDIA vGPU.	
37.	The hypervisor software must be fully compatible and certified for the Enterprise GPUs and software	
38.	Must provide sharing of GPU among different virtual machines using vGPU	
39.	Must provide for allocation/scheduling of physical GPU to virtual machines	
40.	Must include 2 nos. of high-performance low-latency network switches with Layer3 feature set, 24 or more ports per switch, redundant power supplies and cooling fans. The switches must be provided with sufficient 25Gbps SFP28 populated ports and bandwidth for downlink ports and minimum 4 x 40G QSFP populated ports for uplink connectivity. All required SFPs, transceivers and licenses to be provided. The switches must be fully compatible and tightly integrated into the HCI solution for maximum performance.	
41.	The switches must be fully compatible and tightly integrated into the HCI solution for maximum performance	
42.	All required cables and connectors for connecting all HCI nodes to switches in redundant mode to be supplied	
Management		
43.	Must provide client authentication using protocols and directory services such as LDAP and Active Directory	
44.	Solution should provide Kubernetes in the control plane of hypervisor for unified control of compute, network and storage resources to run both containers/native pods and virtual machines on the same platform	
45.	Must provide Role Based Access Control to enable fine grained access control and management of resources	
46.	Must have comprehensive tools to manage clusters and monitor health from the same console	
47.	Multi cluster virtual machines and storage management from a single console	
48.	Must have in-built support for Rest APIs to provision, manage, access and utilize the resources	
49.	Must provide a HTML5 User Interface, SNMP v3 monitoring, SMTP alerts, analysis of alerts	
50.	Must provide dashboard to manage and provision virtual machines, network & storage, monitor performance and manage events, logs & alerts	
51.	HCI solution should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues	
52.	Must allow updates of hypervisor and SDS without any virtual machine downtime	
53.	The HCI must provide seamless non-disruptive upgrade for system firmware, hypervisor, SDS software, management software and other software provided by HCI Vendor	
54.	All hypervisor, SDS, management, vGPU and other software licenses supplied should be perpetual	



55.	The network virtualization should provide distributed in-kernel routing (OSPF & BGP) or virtual routing VXLAN based or similar logical virtual switching, NAT function, server load balancer, If this functionality is not available within solution then vendors can integrate with third part OEMS solution.	
56.	Solution should be able to deliver heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility. It should also provide deep operational visibility and faster troubleshooting across physical, virtual environments. If this functionality is not available within solution than vendors can integrate with third part OEMS solution	
57.	Solution should be able to collect and analyze all types of machine-generated logdata and able to connect it to everything in the environment—operating systems (including Linux and Windows), applications, storage, firewalls, network devices or something else—for enterprise-wide visibility via log analytics.	
58.	The solution should have the ability to deliver end to end security for all applications by delivering network-level micro-segmentation, distributed firewalls, load balancers, virtual routers, virtual switches, compute-level encryption for VM, hypervisor, and live migration. If this functionality is not available within solution than vendors can integrate with third part OEMS solution.	
59.	Solution should have OpenStack Orchestration, K8s service is included in the solution without any additional charges, K8s cluster management with Cluster Autoscaler support, K8s rolling update with the ability to select the specific worker group VPN service included, High-performance S3 support, The ability to configure QoS (IOPS, MB/sec) per specific storage policy with automatic QoS scaling depends on volume size, Self-service UI with the ability to manage all infrastructure services and OpenID integration, Integrated monitoring solution with custom dashboards, NFS storage support, iSCSI storage support	

### 7.3.9 Server Type I

Sr. No.	Item	Specifications of Server (Type-I)	Compliance (Yes / No)
1.	Processor	2xIntel Xeon Gold 3rd Generation / AMD EPYC 32cores, 2.8 GHz or higher.	
2.	Memory	512GB, DDR4 - 3200 MHz ECC memory or higher	
3.	Hard Disk	2x900 GB NVMe SSD and 4x2 TB SAS 10K or higher	
4.	RAID Controller	Should support dedicated 12Gbps RAID controller. It should support RAID 0,1,5,6.	
5.	Storagemodule	PCIex8-1 No, PCIex16- 2 No. or higher	
6.	Power Supply	Dual, Hot-plug, Redundant Power Supply.	
7.	Network Interface	2x10 Gbps Ethernet Base-T and 2x25 Gbps SFP28 for interfaceand populated with transceivers	
8.	FC Interface	2x32 Gbps FC HBA populated with SFP modules.	
9.	USB Drive	Yes	
10.	Form factor	2U Rack mountable	

11.	Terms & conditions	The vendor should be an authorized partner of the OEM.	
-----	--------------------	--------------------------------------------------------	--

### 7.3.10 SAN Switches

Sr. No.	Specifications of SAN Switch	Compliance (Yes / No)
1.	Minimum Dual SAN switches shall be configured where each SAN switch shall be configured with minimum of 24 x 32Gb Ports. 24 x 15M FC Cables to be provided.	
2.	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only	
3.	Should deliver 32Gbps non-blocking architecture with 1:1 performance for up to 24 ports in a energy-efficient fashion	
4.	Should protect existing device investments with autosensing 8, 16, and 32 Gbit/sec capabilities.	
5.	The switch shall support different port types such as E_Port, D_Port, AE_Port, F_Port & EX_Port	
6.	The switch should be rack mountable	
7.	Should provide enterprise-class availability features such as redundant and hotpluggable components like power supply and FAN	
8.	The switch shall provide Aggregate bandwidth of 768 Gbps end to end.	
9.	Offered switch shall not have latency more than 700 ns for locally switched ports.	
10.	Offered switch shall support at-least 15000 frame buffers with dynamic buffer sharing capability across ports.	
11.	Switch shall have support for web-based management and should also support CLI.	
12.	The switch should have USB port for firmware download, support save, and configuration upload/download.	
13.	Offered SAN switches shall be highly efficient in power consumption. Bidder shall ensure that each offered SAN switch shall consume less than 250 Watt of power.	
14.	Switch shall support POST and online/offline diagnostics, including RAS trace logging, environmental monitoring, non-disruptive daemon restart, FCping and Pathinfo (FC traceroute), port mirroring (SPAN port).	
15.	Offered SAN switch shall support services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expedite high- priority traffic	
16.	The switch shall be able to support ISL trunk up to 256 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.	
17.	SAN switch shall support to restrict data flow from less critical hosts at pre-set bandwidths.	
18.	It should be possible to isolate the high bandwidth data flows traffic to specific ISLs by using simple zoning	
19.	The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a	

	single fabric.	
20.	Offered SAN switches shall support to measure the top bandwidth-consuming traffic in real time for a specific port or a fabric which should detail the physical or virtual device.	

### 7.3.11 NVMe SSD storage

Sr. No.	Specifications of NVMe SSD storage	Compliance (Yes / No)
1.	The storage system with standards based on NAS/SAN functionality with all flash NVMe array. All subsystems of the storage like heads, controllers, storage arrays, OS, NAS/SAN software's etc. must be fully inter-compatible and provided & supported by the same OEM.	
2.	It must have minimum dual redundant controllers in active-active mode with automatic fail over to each other in case of failure.	
3.	The storage array needs to be enterprise storage in terms of performance, scalability, features and functionalities. The proposed array should deliver minimum 600000 IOPS with latency of less than 1 milli sec and 5 GBps throughput. SI need to submit benchmark and undertaking for the same. The above performance figures are considering 100% reads for an average IO size of 8KB to the Flash systems and without considering any caching effects. This should be supported undertaking from the OEM on the above performance.	
4.	Required usable capacity is 100TB for files after taking into consideration any space required for spares, and parity. Above capacity mentioned are usable capacities to be configured under RAID-6. Spares / additional capacity to be configured by the OEM. The required capacity should be met with delivered using NVMe Flash Drives.	
5.	The storage array should guarantee no data loss in the event of a power failure in the data centre and a component failure in the storage array. The proposed storage system should have the ability to back up the Cache information into non-volatile storage in the event of any outage or failure to the system to protect against data loss.	
6.	Storage array shall support hot plugging and hot swapping of all components on-line (i.e., disks, cache boards, power supplies, cooling fans, microcode updates) with no disruption to any applications or loss of data.	
7.	The Storage Management Software shall be GUI based and shall be able to discover and monitor storage system. It shall provide pro-active intelligence by monitoring performance of Storage Infrastructure.	
8.	Storage should have performance monitoring software which is an automated, intelligent and path-aware storage resource management tool that maps, monitors, analyzes and measures storage network resources and performance from the application to the device.	
9.	Should come pre-installed with the OEM certified OS with perpetual license	
11.	Interface: Front-end connectivity with 4 x 25Gb SFP28 MM Ethernet ports per controller. Backend connectivity with NVMe	
12.	The supplied equipment must work with 230V, 50 Hz AC power supply with Indian type power outlets. Necessary adapter to be provided by the vendor if	

	required.	
--	-----------	--

### 7.3.12 Unified Storage System

Sr. No.	Specification for Unified Storage System	Compliance (Yes / No)
1.	The Storage Solution should be based on controllers with Data Assurance in active-active mode configured in a NSPOF and End-to-End Data Protection.	
2.	The storage should be configured with NFS / CIFS / FC / iSCSI protocols. Any hardware / software required for this functionality shall be supplied along with it in No Single Point of Failure mode.	
3.	The system should have minimum 1 TB cache memory across the two controllers with an ability to protect data on cache during controller / power failure. The cache on the storage should have battery backup. Cache should be scalable to 2TB considering future growth without replacing the existing controllers.	
4.	The storage array needs to be enterprise storage in terms of performance, scalability, features and functionalities. The proposed array should deliver minimum 300000 IOPS and 3 GBps throughput. SI need to submit benchmark and undertaking for the same.	
5.	Storage should support RAID 6 or equivalent	
6.	Storage should be supplied with 1PB usable capacity (200TB SSD and 800TB of NL-SAS) with RAID6 and scalable. Usable capacity should be considered after taking all overheads.	
7.	The storage should be supplied with rack mount kit. All the necessary patch cords (Ethernet and Fibre) shall be provided and installed by the vendor.	
8.	The storage shall have the ability to expand LUNS / Volumes on the storage online and instantly.	
9.	The storage shall have the ability to create logical volumes without physical capacity being available or in other words system should allow over-provisioning of the capacity. The license required for the same shall be supplied for the maximum supported capacity of the offered storage model.	
10.	The required number hard disks for parity & spares, should be provided exclusively of the usable capacity mentioned after considering RAID and Filesystem overhead. At least 2% of the usable capacity requested on each tier should be configured as spare drives with the subsequent disk types.	
11.	The proposed storage system should be configured to provide data protection against two simultaneous drive failures.	
12.	System should have redundant hot swappable components like controllers, disks, power supplies, fans etc.	
13.	Support for industry-leading Operating System platforms including LINUX, Microsoft Windows etc.	
14.	The proposed storage system should have: 4x 25 Gbps SFP28 MM + 4x 32 Gbps FC ports available per controller.	
15.	Must have thin provisioning and data encryption.	

### 7.3.13 Backup Storage System & Software

Sr. No.	Specifications of Backup software, Backup server and Storage	Compliance (Yes / No)
1.	The Storage Solution should be based on multiple controllers with Data Assurance in active-active mode configured in a NSPOF and End-to-End Data Protection.	
2.	The storage system with standards based on NAS/SAN functionality	
3.	The storage should be configured with NFS/CIFS/FC/iSCSI protocols. Any hardware / software required for this functionality shall be supplied along with it in No Single Point of Failure mode	
4.	The system should have minimum 256 GB cache memory across multiple controllers with an ability to protect data on cache during controller/power failure. The cache on the storage should have battery backup. Cache should be scalable to 2TB considering future growth without replacing the existing controllers.	
5.	Should support RAID level 6	
6.	Storage should be supplied with new 1.2PB of NL-SAS usable capacity with RAID6 and scalable. Usable capacity should be considered after taking all overheads.	
7.	The proposed storage system should have 4 x 25 Gbps ports available per controller.	
8.	The storage should be supplied with rack mount kit. All the necessary patch cords (Ethernet and Fiber) shall be provided and installed by the vendor.	
9.	The storage shall have the ability to expand LUNS/Volumes on the storage online and instantly.	
10.	The storage shall have the ability to create logical volumes without physical capacity being available or in other words system should allow over-provisioning of the capacity. The license required for the same shall be supplied for the maximum supported capacity of the offered storage model.	
11.	The required number hard disks for parity & spares, should be provided exclusively of the usable capacity mentioned after considering RAID and Filesystem overhead. At least 5% of the usable capacity requested on each tier should be configured as spare drives OR spare capacity with the subsequent disk types.	
12.	The proposed storage system should be configured to provide data protection against two simultaneous drive failures.	
13.	System should have redundant hot swappable components like controllers, disks, power supplies, fans etc.	
14.	Support for industry-leading Operating System platforms including LINUX, Microsoft Windows, IBM-AIX, etc.	
15.	The Hardware and software quoted should have 5 years support along with upgrade and updates.	
Specification of Backup Server		
16.	Processor: 2x Intel Xeon third generation 8 core, 2.8 GHz, 12 MB cache	
17.	Memory: 128 GB DDR4 3200 MHz Memory or higher	
18.	HDD: 2 x 800GB PCIe M.2 module & 4 x 800 GB SAS 10K Read/Write SSD Drive, Disk should be of 12 Gbps backend	
19.	RAID Controller: RAID card supporting RAID 1, 5, 6, 10. It should be provided with 512 MB cache, battery backup for zero data loss.	

20.	Network Interfaces: 2 x 10 Gig Ethernet Base-T, 2 x 16Gb HBA and 1x 1Gig port for management	
21.	Operating System: License version of Microsoft Windows Server 2022 64 bit or higher / latest	
Specification of Backup Software		
22.	Proposed solution support backup of various OS platforms like Windows, Linux etc. The proposed solution should have integrated view of backup and replication.	
23.	The offered software must include application aware backups for Oracle, MySQL, PostgreSQL, MS SQL, etc.	
24.	The software must keep single copy for backup with the help of de-duplication across different electronic data repository for storage optimization.	
25.	The proposed solution must have capability to protect the backed-up disk volume from Ransomware with WORM capabilities.	
26.	The software must be able to compress and encrypt data at the Client-side and this feature should be available even during de-duplication.	
27.	Proposed software should have intelligent integration with different storage vendors snapshots to provide Application consistent backup copy.	
28.	The offered software should support Industry Standard Encryption algorithms for data protection.	
29.	The offered software solution should include capability to archive data based on retention as per the requirement of business units.	
30.	The offered software must support backup data archival with seamlessly for any type of data residing on Windows/Linux OS.	
31.	Solution should have the ability to archive and allow utilization of any type of target repository for backup and archive to achieve space efficiency and easier data management	
32.	Backup software must support both source side and target side deduplication capability.	
33.	End user must have provision to access their backup data and perform restore operations from their own devices	
34.	The software should be capable to take the back up for End-users.	
35.	The backup software license should be offered for 100 TB Backup capacity.	
36.	The proposed backup software should provide Instant recoveries to the physical and virtual infrastructures.	
37.	Backup software should be able to work in high availability cluster mode in physical / virtual server. Required license to be enabled.	

#### 7.3.14 Rack, KVM Switch and Console

Sr. No.	Specifications for 42U RACK/KVM Switch and Console	Compliance (Yes / No)
Rack, PDU and Console		
1.	19" 42U Server Rack Attractive Styling for Data Centre (800mm Width x 1000mm Depth)	
2.	Basic Frame: MS CRCA Sheet Steel as Industry Standard.	

3.	Top & Bottom cover bolted to frame with cable entry exit cut outs.	
4.	Front Door Lockable, Steel/Vented/Perforated.	
5.	Rear Door Lockable, Steel/Vented/Perforated.	
6.	19" Mounting Angle Required at front and rear.	
7.	Standard finish powder quoted. All round accessibility.	
8.	Standard color grey/black	
9.	Heavy Duty mounting caster wheels load rating 1000 KGS (2 with brake & 2 without brake) or levelers or plinth.	
10.	K/B Mouse with sliding monitor (Rack mounted)	
11.	Two Nos Vertical PDU 5 / 15Amp with 12 Socket with 3meter Cable and locking IEC Cords solution to secure equipment's power cables c13 to c14 compatible pdu's.Intelligent PDUs with power monitoring features	
12.	Stationery Shelf 700mm - 6 No	
13.	Support Angles 700mm required	
14.	Rack mount console with Flip up LCD monitor (FHD 1920x1080) usb keyboard in 1RU.	
15.	Cable Channel 42U - 6 Nos	
16.	Earthing Kit and mounting hardware should be provided	
17.	With the required accessories to fit all computing systems being procured as a partof consolidated proposed RFP purchase.	
18.	The racks and all other required accessories must have 24x7 comprehensive onsite warranty, with advanced part replacement, from the OEM with comprehensive warranty of 5 yrs.	
19.	System Integrator should supply a minimum of 6nos. of 42U racks with features asfollows: The front door and rear door must have perforation pattern; the rear door should be split.	
20.	Split type side panels with single point locking and quick release latches.	
21.	The racks must include cable manager, Earthing kit, casters and levelers, and other required accessories	
22.	Rack must comply with the standards either UL 60950-1 or EIA-310.	
23.	The PDUs and power cables must be in compliance with the industry standards.	
24.	All the power cords, C13 toC14, should be with 90 degrees Left and Right, lockable,must be factory integrated.	
KVM		
25.	Dual Console operation: system can be control from both the local and remotekeyboard, monitor and mouse console.	
26.	Built-in ASIC for greater reliability and compatibility	
27.	Built-in 8KV/15KV ESD Protection (Contact Voltage 8KV; Air Voltage 15KV) and 2KV surge protection.	
28.	Support VGA, SVGA, SXGA (1280X1024), UXGA (1600X1200), WUXGA (1920X1200) and multi sync monitors; local monitor supports DDC; DDC2; DDC2B	
29.	Hot Pluggable, Rack Mountable	
30.	OS Support: Should support all OS	
31.	Computer connections: 4 or more	

32.	Console Keyboard connector: 2XUSB Type A	
33.	Console Mouse connector: 2XUSB type A	
34.	Console PS/2 to USB Adapter Cable: 2 x PS/2 for mouse and keyboard to 1 x USB Type A	
35.	Console Video Connector: 2 x VGA-15 pin female	
36.	Console Audio Connectors: 2 x Mini-DIN Speaker Port (rear of switch), 2 x MiniDIN Microphone port (rear of switch)	
37.	CPU KVM Connectors: Connectors are used for attaching the custom cables sets that link the switch to the computers. KVM data: 4 x SPDB - 15 pin female (rear of switch)	
38.	Scan Interval: 1 - 99 secs. (5 secs. default)	
39.	Resolution: Minimum of 1920x1080 pixels.	

### 7.3.15 LED Monitor with compatible adapter, cables, and wall mount kit

Sr. No.	Specifications for LED Monitor with compatible adapter, cables, and wall mount kit	Compliance (Yes / No)
LED Screen		
1.	LED screed Shall be quoted with all accessories, connectors, cables, stand and wall mounting kit.	
2.	Screen size: 59 Inch or more	
3.	Resolution: min resolution of 3840 x 2160 or above	
Matrix and switching equipment for connecting management servers to display panels		
4.	Eight (8) inputs and eight (8) outputs for matrix switching of HDMI or DVI and support HDBaseT extension. All of transmit & receive modules shall be included	
5.	The solution must have the capability that each input can be routed to any output, or the same input can be routed to all outputs or any combination, eliminating the need to manually move cables to display HDMI or DVI video from different sources on different screens.	
6.	Must support easy Switching using front-panel buttons, IR remote controller, or an RS-232 connection or via IP	
7.	Must support a distance of 100 M from the video source to Display Panel.	
8.	Must be Compatible with all HDMI source devices, PC monitors, LED FHD displays, FHD TV, and audio receivers / amplifiers.	
9.	Must work with wide range of FHD resolutions from PC XGA to WUXGA 1920 x 1200 and FHD TV / TV resolutions with FHD.	
All-in-one Desktop machine each with the following specs: - 4 Nos.		
10.	Processor Intel® Core™ i7-12 <sup>th</sup> generation with Intel HD Graphics or better	
11.	Memory, standard: 16 GB 2600 MHz DDR4 or better	
12.	Hard drive: 512GB NVMe SSD module and 1 TB 7200 rpm SATA	
13.	Display 22" diagonal LED-backlit or better	
14.	Network interface: Integrated 1Gbps Gigabit Ethernet LAN	
15.	Webcam: Yes, Integrated Webcam.	
16.	Input / output: Keyboard and mouse	



### 7.3.16 Host Intrusion Prevention System (HIPS)

Sr. No.	Specifications of Host Intrusion Prevention System (HIPS)	Compliance (Yes / No)
1.	Should support following all leading operating systems, including Microsoft Windows, Cent OS, Oracle Linux, Red Hat Enterprise Linux, SUSE Linux, Ubuntu. The solution should offer next generation antivirus with machine learning, firewall, threat intelligence, Application Control, File Integrity monitoring, Log inspection and , customized virtual sandbox for zero-day threat protection, HIPS / Threat Prevention, Virtualization Security, and cloud workload solutions RG in a single agent functionality to ensure optimal security and compliance for critical servers both on premise and cloud-based deployments.	
2.	Should provide automated, real-time intrusion detection and protection by analyzing events, operating system logs and inbound / outbound network traffic on enterprise servers along with recommendation for automatic removing of assigned rules if a vulnerability or software no longer exists such as patch is deployed or AD software is uninstalled.	
3.	Analyze all packets to and from the server for and propagation to detect and prevent attacks, both known and unknown intrusion attempts.	
4.	Should prevent the delivery and installation of kernel-level Root kits. Should prevent cross-site scripting (XSS) attacks, SQL injection attacks, DOS, DDOS, worm, bot, botnet, Trojan attacks, Buffer overflow attacks, should decode backdoor communications and protocols. Should employ full, seven-layer, state-based protocol decoding and analysis. Should employs network-level, vulnerability-centric signatures/algorithms. Should identify and alerts on user activity, including user account creation,deletion, and modification.	
5.	Should identify and alerts on group activity.	
6.	Should identify and alerts on file activity, including file additions, deletions, content changes, and ownership changes.	
7.	Enforces operating system audit policy/event monitoring and must have an option of automatic recommendation of rules for log analysis as per the Server OS which can be scheduled for automatic assignment/unassignment of rules when not required. Should support decoders for parsing the log files being monitored with customized sdk rule creation supporting pattern matching like Regular Expressions or simpler String Patterns.	
8.	Should encompass a wide array of built-in alerting, blocking, and logging responses for each event. List all available responses.	
9.	Should enable / disable each individual signature or group of signatures based on various criteria, such as type and severity	
10.	Agents are managed by a central administration system designed for large- scale enterprise deployments	
11.	Should support central management of policy configuration and one-touch, global policy roll- out for policy changes and application	
12.	The license should be provided for 40 applications	

### 7.3.17 Endpoint Detection and Response (EDR)

Sr. No.	Specifications of Endpoint Detection and Response (EDR)	Compliance (Yes / No)
General Features		
1.	The solution should have all its components deployed on premise	
2.	Solution should NOT share any data of endpoints i.e. telemetry details in public cloud.	
Management Console		
3.	The solution should provide a unified web-based console for all functionalities and should allow administrators to access the management interface from any authorized machine, without installing additional software.	
4.	Solution should provide a console easy to understand and to navigate with common workflows.	
5.	The proposed solution must have the option to create role based access/view(s) of the management console.	
6.	Solution should support multi-factor authentication for the management console	
7.	Solution should provide Centralized auditing and logging of activity is maintained in the management console.	
Agent Capabilities		
8.	Solution should provide strong anti-tamper capabilities, to ensure that an end user can not remove, disable or modify the product in any way.	
9.	Solution should have ability to upgrade agents with no impact to the end users.	
10.	Agent to be uninstalled remotely from the management console.	
11.	Deployed agents must be able to communicate with central management server via a web- proxy.	
Operating System Support		
12.	Solution must support all supported versions of Operating Systems and should continue support for a minimum period of 12 months after the OS version is end of sale/life.	
13.	Solution must support all the latest versions of Windows Operating Systems. Following but not limited to: Windows Server Core 2016 and 2019 Windows Server 2022, 2019, 2016 Windows 10, 11	
14.	Solution should support all the latest Linux environments CentOS, Debian, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server, Ubuntu	
Threat Prevention		
15.	The proposed solution should provide context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. The solution must have feature for Custom detection, intelligence, and controls.	
16.	EDR Solution must provide prevention across all major Operating Systems – Windows, MacOS and Linux.	

17.	EDR Solution must have capability to protect the system against known and unknown malwares.	
18	EDR solution should ensure that every read, write and execute operations on files is checked for malware	
19.	Solution should be effective against sophisticated attacks by analyzing Behaviors on an endpoint, along with signature based approach.	
20.	The solution should allow the user to perform threat hunting to detect dormant threats as well.	
21.	The EDR solution should support protection capabilities across Windows, Mac, Linux	
22.	Solution must provide prevention across ALL major Operating Systems – Windows, MacOS and Linux.	
23.	The solution should protect endpoints from malicious documents and scripts.	
24.	The solution should monitor and protect the system from lateral movements & insider threats.	
25.	The EDR solution should monitor and protect from exploits and file-less attacks.	
26.	The EDR solution should identify and block potentially unwanted programs on the systems.	
27.	The alerts should be correlated together automatically if related to the same attack.	
Response & Remediation Capabilities		
28.	The proposed solution should provide option to sweep and assess the current (point in time/Live) state of the devices. 1. Scan disk Files 2. Scan in memory process 3. Search registry	
29.	The proposed solution to provide the advance response capabilities as mentioned below 1. Kill process 2. Isolate device 3. Block process	
30.	The proposed solution can take risk based response on the endpoint based on endpoint characteristics and reputation. The reputation of the endpoint is computed based on unusual or malicious behaviour of endpoint over time.	
31.	Solution should alert on both suspicious and malicious threat behavior.	
32.	Solution should have ability to kill and quarantine an offending process.	
33.	Solution should provide option to network quarantine a device and provide flexibility to configure the same.	
34.	Solution should have options to add notes or set the status of an issue or event (i.e. resolved, in progress, unresolved)	
Policy & Installation		
35.	Tool should provide Ability to support policy propagation across an account, site or group of devices	
36.	Tool should include clauses to easily exclude false positives	

37.	Tool should provide the option for the administrators to make policy exclusions of the console at multiple levels? (Account, Group)	
38.	Provide exclusions set at process level	
39.	The product should stream EDR data in real-time to own internal data lake for Threat Hunting purposes	
40	EDR solution should natively send event logs via Syslog. The solution must support the following syslog formats: CEF, LEEF	

### 7.3.18 Network performance Monitoring & Diagnostics (NMS)

Sr. No.	Specifications of Network performance Monitoring & Diagnostics (NMS)	Compliance (Y / N)
1.	The proposed monitoring solution should be able to monitor all the devices deployed as a part of MRSAC on-prem data center, including but not limited to: Routers, Switches, LLB, SLB Other SNMP-enabled devices, along with UPS, PAC, IPPDUS's, Energy meters. The OEM should be Make-in-India and startup resgitered and from the same OEM as the EMS, SIEM and Asset management tool.	
2.	Should automatically provide real-time, in-depth network performance statistics after discovery/configuration of devices, including but not limited to:(a) CPU load (b) Memory utilization © Interface utilization (d) packet loss	
3.	Should show statistics like interface bandwidth, current traffic in bps, total bytes received/transmitted etc.	
4.	Should be able to discover and troubleshoot network paths hop- by-hop for specific TCP connections	
5.	Should display information including alerting for major routing protocols (BGP, OSPF, RIP) with options to view and search routing tables including VRFs, changes in default routes and flapping routes, router topology and neighbor status	
6.	Should help with multicast traffic information monitoring, alerting including topology information, multicast information, route information, multicast errors etc.	
7.	Should display device status and interface status by different colors to represent warning and critical status	
8.	Should show both real-time details and historical details in form of charts with option to choose the time periods	
9.	Should be able to discover and monitor both IPv4 and IPv6 devices	
10.	The proposed monitoring solution should be able to discover devices in the network with SNMP and ICMP capabilities	
11.	Should not add devices with multiple IP addresses as duplicate nodes but should list all known IP addresses for the node	
12.	Should allow interface filtering on discovery results to exclude virtual interfaces and access ports and select interfaces based on pattern matching	
13.	Should be able to automatically imports discovered devices	
14.	The proposed management solution should provide a high-quality graphical user interface with asynchronous view refreshing	
15.	This web console should be accessible centrally or remotely	

16.	The web console should allow multiple users to log in at the same time	
17.	It should have load-balancing options available if too many users' login at same time	
18.	It should allow customization by having options to add / remove sections in web pages as necessary	
19.	It should provide a unified view of alerts, traps, events, syslog messages in a single page	
20.	It should give a single unified view of multicast information, route information and device information for a device.	
21.	It should quickly highlight devices with issues, based on different properties like response time, CPU load, memory usage, high interface usage etc.	
22.	It should allow creation of custom dashboards and restrict views for users based on devices or interfaces, i.e., it should have role-based access	
23.	It should log user actions and events in the web console for audit purposes and they should be available for alerting and reporting	
24.	It should allow interactive charting for node, interface, volume charts etc.	
25.	It should provide a dynamic dashboard that allows in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable with a tabular format	
26.	The proposed monitoring solution should provide current and historical out-of-the-box reports for various statistics monitored	
27.	Should be able to generate / create the report via the web console	
28.	Should be able to generate statistical reports that can be used as reference for future planning or troubleshooting	
29.	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.	
30.	Should allow advanced customization by providing options to enter custom queries to query the database directly	
31.	Should have options to save the customized reports permanently and have them accessible in web console	
32.	Should allow reports to be sent out on schedule as daily, weekly, monthly report	
33.	Should be able to configure both charts and tables into a single report.	
34.	Should have options to import / exports reported created by other users	
35.	Should support multiple formats such as pdf, HTML and CSV	
36.	The alerts and events information should be logged into the database for future reference	
37.	The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition	
38.	It should allow custom queries to be entered to create rules against the database	
39.	Should have support for variables in alert email message to make the content more self explanatory	
40.	Should have the ability to dynamically baseline statistics and automatically set Warning and Critical threshold	
41.	The proposed monitoring solution should allow grouping of devices by various properties -- by department, by location, by name and by other properties gathered	
42.	Should be able to define dependencies and relationships between connected devices and interfaces to avoid false-positive email alerts in case of outage.	

43.	The proposed monitoring solution should be able to represent the network pictorially and display performance details of devices in real time. Should allow customization of background, icons etc	
44.	Should be able to display not just the device status on the map but also status of any other detail obtained.	
45.	Should be able to automatically connect devices by means of topology information gathered during discovery	
46.	Should have the ability to show the link utilization	
47..	The solution and its data store should support physical and virtual environment of deployment.	
48.	Traffic and bandwidth usage monitoring, BW capacity monitoring, free upgradation to higher version within support period.	
49.	With a centralized operations console view, alert acknowledgement and reporting interface	
50.	The proposed NMS solution must be from the same OEM offering EMS & Asset Management.	
51.	The license should be provided for 400 devices which should be perpetual. (Minimum 150Vms and 50 Network devices license should be ensured)	

### 7.3.19 Enterprise Management Software (EMS)

Sl. No.	Specifications of Enterprise Management Software (EMS)	Compliance (Y / N)
1.	The proposed solution should be an on-premises solutions. The proposed EMS solution either be from the same OEM or should be tightly integrated with NMS & Asset Management for unified dashboarding and reporting. And NMS OEM Should be CMMI L3 certified with ISO 9001, ISO 14001, ISO 27001, ISO 27034 as well as IATF 16949 and registered under MSME and recognized by govt as startup under the startup India programme. EMS, NMS, Asset management, SLA management, IPAM, SIEM, Policy compliance and obsolescence management, knowledge management, threat alert mechanism from the same OEM.	
2.	The proposed solution must be able to perform infrastructure aware application triage, i.e., pinpoint network issues causing application degradation.	
3.	The proposed solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view	
4.	The proposed solution must proactively monitor 100%of real user transactions; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes	
5.	The proposed solution must provide complete end-to-end transaction visibility by monitoring at a transactional level and without deploying any software at end user desktop.	
6.	The proposed solution must provide a single view that shows entire end-to-end real user transaction and breaks down times spent within the application components, SQL statements, backend systems and external 3rd party systems.	

7.	The proposed solution must provide a real-time application topology map to triage and quickly pinpoint the component causing a performance bottleneck in the end- to- end transaction flow.	
8.	The proposed solution must gather available performance indicator metrics from all within real-time production environments and real user transactions 24x7 with minimal overhead on monitored applications without sampling.	
9.	The proposed solution must provide for easy dynamic instrumentation of application code, i.e. be able to enhance out of the box monitoring with extra monitoring definitions without having to restart application or JVM/.NET Worker Process.	
10.	The proposed solution must be able to detect production Memory Leaks from mishandled Java collections and sets and isolate exact component creating leaking collection or Set (or .NET Memory Leaks within the CLR).	
11.	The proposed solution must allow monitoring granularity of no more than 1 minute for all transactions.	
12.	The proposed solution must report of response times of Java/.Net methods based on simple method parameters (Strings, Integers etc.).	
13.	The proposed solution must provide real-time monitoring of resource utilization like memory usage, DB connection pools and Threads.	
14.	As a means of detecting poorly performing SQL, the solution must be able to proactively record all SQL calls, and report on the slow performing ones. The SQL measurements must be made from within the monitored application – not using an external database agent.	
15.	The solution should have provision for automatic transaction discovery, for example by setting up some bounding parameters to describe transactions like the web site, the language, and parameters (such as post, query, and cookies).	
16.	The proposed solution must provide ability to monitor performance of applications up to the method level of execution (Java / .Net method) 24x7 in production environments with negligible impact on monitored application.	
17.	The proposed solution must be able to report on any application errors occurred while executing application functionalities and pinpoint exact place of error within transaction call stack.	
18.	The proposed solution must provide for at least two levels of thresholds which can be set on alerts and provide for actions so that alerts can automatically trigger other processes when thresholds are breached. The proposed solution must not necessitate any changes to application source code.	
19.	The proposed solution must proactively identify any thread usage problems within applications and identify stalled (stuck) threads.	
20.	Correlation of the performance inputs from all the 3 application tiers (web, app, and DB) should be achieved from the tool.	
21.	The proposed solution must monitor individual web service and performance transaction debugging for web services. The proposed solution must also monitor web services across multiple processes (cross JVM tracing)	
22.	The proposed solution should eliminate problem resolution guesswork by using its performance metrics to automatically identify complex emerging performance issues, enabling triage and diagnosis teams to solve problems faster and understand their environments better.	
i. End User Experience Management Systems		

1.	The proposed solution should measure the end users' experiences based on transactions without the need to install agents on user desktops.	
2.	The solution should act as a passive listener on the network thus inducing zero overhead on the network and application layer.	
3.	The proposed system must be able to detect user impacting defects and anomalies and reports them in real-time: a. Slow Response Time b. Fast Response time c. Throughput. Partial Response. Missing component within transaction	
4.	The proposed system must be able to provide the ability to create user groups based on application criteria or location and link user ids to usernames and user groups.	
5.	The proposed system must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period such as current week versus previous week.	
6.	The proposed system must be able to provide the ability to detect and alert when	
7.	The proposed solution should be capable of identifying the problem domain (browser, network, or application) thereby it should monitor the browser side metrics and provide reports in real time for: a. Page Load Time (ms), b. Previous page unload time (ms), c. Browser Render Time (ms), d. Page Roundtrip Time (ms), e. Responses Per Interval (browser activity)	
8.	The proposed solution must be able to provide real time transaction health metrics and end user experience quality metrics anytime, anywhere for the business executives.	
9.	The proposed solution must be able to provide the flexibility to select, organize and monitor real time business indicators with the help of an interactive user interface	
10.	The proposed solution must be able to provide flexibility by enabling addition of annotations to business indicators to enhance clarity and context around its behavior enabling better information sharing and collaboration.	
11.	The proposed solution must be able to maintain centralized control of data and security of the data that is viewed on the smart devices like i-phone, i-pad etc.	
ii. General Monitoring Platform		
1.	The Monitoring Solution should provide End to End Monitoring of Complete IT Infrastructure including Network Monitoring, Server Monitoring, Application Monitoring, End User Experience Monitoring, Database Monitoring, Virtualization Platform Monitoring, Storage Monitoring	
2.	The proposed solution should be capable to provide hybrid monitoring architecture through agent/agent less approach and should be able to get data from all industry standard protocols including SNMP, TCP/IP, BACNET, MODBUS, Restful API for monitoring non-IT as well as It equipment's and application.	
3.	The Platform must support Event Correlation Alerting (ECA) integrations to trigger automated creation of incidents, problems, and changes based upon alarms and events correlation.	
4.	The proposed monitoring solution should provide capability to integrate with hardware monitoring platforms.	



5.	The proposed monitoring solution should possess the inherent capability to leverage API's and SDKs to enable integration and monitoring	
6.	The proposed monitoring solution should have capability to configure actions-based rules for set of pre-defined alarms / alerts enabling automation of set tasks.	
7.	The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: Event filtering, Event aggregation, Event masking	
8.	The Reporting Portal should be Completely web based with ability to define Accounts and Users for Role Relevant Views	
9.	The proposed solution should provide the ability to create custom dashboards with ability to aggregate metrics from all monitored devices and should provide drill down functionality to other defined dashboards within the tool.	
10.	The proposed solution should provide ability to monitor and generate alarms for set threshold for pre-defined Service level agreement for monitored metrics. The proposed monitoring solution should provide one-touch upgrade functionality for latest updates and support for new functionalities.	
11.	All the required modules either should be from same OEM or should be tightly integrated for single pane of glass view of enterprise monitoring.	
iii. Server Monitoring Requirements		
1.	The Solution should monitor heterogeneous operating systems for both physical and virtual environments OS including but not limited to Windows 32/64 bit, All Major Flavors of Linux, Solaris, Unix etc.	
2.	The solution should be able to monitor non-SNMP devices (e.g. using WMI, Telnet, SSH etc.)	
3.	Solution should be able to provide end to end observability & correlation till log level.	
4.	The solution should monitor File System Mounts for presence/absence/ functionality	
5.	The solution should have the ability to do "baseline" performance metrics and determine normal operating values and patterns by self- learning algorithms on a day, week, month, etc. and ability to configure threshold on these values. The solution should also have built in algorithms to start the monitoring with zero threshold configurations	
6.	The solution should support monitoring log files. The solution should support monitoring of Windows Event Logs and provide correlation of events for these.	
7.	The solution should support monitoring of performance counters in Windows /Linux environment	
8.	The solution should support monitoring of services / processes in a Windows /Linux environment.	
9.	Processes monitoring should also have ability to track CPU and Memory consumption of the monitored process for alerting and reporting / trending purpose.	
10.	The solution should report on services not in the expected state and \optionally start or stop them.	

11.	The solution should support the monitoring of processes & taking automated actions	
12.	The solution should support monitoring new processes that come up on a server.	
13.	The solution should support monitoring CPU performance over defined user defined time periods of time	
14.	The solution should support monitoring Availability and performance of memory, including upper and lower thresholds and types of usage	
15.	The solution should support monitoring Local and Attached Disk capacity and provide delta change in used capacity	
16.	The solution must monitor the availability, health, and performance of \Microsoft	
17.	The Solution should Monitor automatic reboots of servers	
18.	The Solution should support monitoring new processes that come up on a server	
19.	The proposed EMS solution must provide agentless as well as agent-based monitoring for server infrastructure. The agents should be able to set polling interval as low as 1 second with low overhead on target server infrastructure	
iv. Database Monitoring Requirements		
1.	The solution should monitor multiple database servers and multiple versions of each server including Oracle/SQL Server/Informix/DB2/Sybase/Postgres/MySQL etc. Including database proposed by MSP	
2.	The Solution should Provide SQL Response Time for Monitoring Custom Queries	
3.	The Solution should provide response time Monitoring for custom queries through JDBC Mechanism to allow monitoring unsupported databases	
4.	Database Space Monitoring for both file group and transaction log (Warning threshold, Critical threshold as well as file group/log full)	
5.	Performance monitoring - capture of DB Engine related performance counters as well as threshold alerting	
6.	The solution must support SQL Agent monitoring - failed jobs, long running jobs	
7.	The solution must support Database Health and Settings - Check database status (offline, suspect), Check database options (auto grow, auto shrink, auto close etc.)	
8.	The solution must support monitoring of Replication, DB Mirroring and Log shipping if applicable	
9.	The solution must be able to report & check for last recent Full database backup and last recent Transaction Log backup	
10.	The solution must monitor for Blocking (exceeding duration) and Deadlocks	
11.	The solution must be able to run power shell, python to perform tests on the database and have the results put into the solution as performance data and or alarms	
12.	Inclusion of SQL statements within the Solution should be a standard “easy-to- use” function achieved without programmatic intervention.	
13.	The solution should support auto-discovery of database instances.	

14.	The solution should support the use of schedules and time filters for database monitoring.	
v. Virtualization Monitoring Requirements		
1.	The solution should provide support for leading virtualization platforms.	
2.	The solution should support monitoring of virtualized through management interface.	
3.	The solution should provide capability to monitor events generated by the hypervisor to generate alarms and alerting functionality	
4.	The Solution support CLI-based network device configuration snapshot management including backup of configuration files, traffic logs, messages etc., pushing configuration files to target network devices, with option to perform remote firmware upgrades.	
5.	The solution should provide a configurable interface to view performance metrics related to virtualization infrastructure	
6.	The solution should provide capability to monitor the availability to Web APIs of application.	
7.	The proposed solution should be integrated with centralized monitoring tool to enable aggregation of alarms and alerts.	
8.	The proposed solution should allow reporting through unified reporting console along with other infrastructure devices being monitored.	
vi. Storage Monitoring Requirements		
1.	The proposed solution should be able to monitor leading enterprise storages through standard interfaces	
2.	The proposed solution should be able to monitor in depth metrics and performance data for supported storage platforms	
3.	The proposed solution should automatically discover storage configuration and auto applies monitoring by template	
4.	The proposed tool should be able to monitor other storage devices through SNMP	
vii. SLA Monitoring Specifications		
1.	General: The solution must support Service Level Agreements Lifecycle Management including Version Control, Status Control, Effectively and audit Trail.	
2.	General: The solution must provide a flexible framework for collecting and managing service level templates including Service Definition, Service Level Metrics, Penalties, and other performance indicators.	
3.	Service Delivery: The solution must have the ability to define and calculate key performance indicators from an End-to-End Business Service delivery perspective.	
4.	Contract Management: The solution must support dependencies between supplier contracts and internal or external contracts.	
5.	Bonus & Penalty: Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs. Support for Defining and Calculating service Bonuses based on clauses in SLAs	

6.	Alerts: The solution must support delivery mechanisms to indicate / notify whether SLA targets are being achieved or violated.	
7.	Dynamic Calculations: The solution supports dynamic service level targets on priority.	
8.	Audit Trails: Full electronic audit trails available for both system and user transactions	
9.	Reporting: Report module and SLA Management module must be integrated to provide ease-of reports configuration and execution.	
viii. Helpdesk Management		
1.	The proposed helpdesk solution must provide flexibility of logging, viewing, updating, and closing incident manually via web interface.	
2.	The web interface console would also offer power-users tips	
3.	The proposed helpdesk solution must provide seamless integration to log incident automatically via system and network management.	
4.	The proposed helpdesk solution must provide classification to differentiate	
5.	The proposed helpdesk solution must be able to provide flexibility of incident assignment based on the workload, category, location etc.	
6.	Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no programming	
7.	The escalation policy would allow flexibility of associating with different criteria like device/asset/system, category of incident, priority level, organization, and contact.	
8.	The proposed helpdesk solution must provide web-based knowledge database to store useful history incident resolution.	
9.	The proposed helpdesk solution must have a strong Business Objects based reporting module built in it.	
10.	The proposed helpdesk solution must integrate with EMS event management and support automatic problem registration, based on predefined policies.	
11.	The proposed helpdesk solution must be able to log and escalate user interactions and requests	
12.	The proposed helpdesk solution must provide status of registered calls to end-users over email and through web.	
13.	The proposed helpdesk solution must have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.	
14.	The proposed helpdesk solution must have the ability to track work history of calls to facilitate troubleshooting.	
15.	The proposed helpdesk solution must support tracking of SLA (service level agreements) for call requests within the help desk through service types.	
16.	The proposed helpdesk solution must support request management, problem management, configuration management and change order management.	
17.	The proposed helpdesk solution must be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.	
18.	Knowledge tools and Configuration Management Data Base (CMDB) should be integral built-in components of Helpdesk and should be accessible from the same login window to enable seamless access.	

19.	The proposed helpdesk solution must allow the IT team to see the Configuration Items (CI) relationships in pictorial format, with a specified number of relationships on single window.	
20.	The proposed helpdesk solution must have a top management dashboard for viewing the helpdesk KPI in graph & chart formats.	
21.	The proposed helpdesk solution must support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.	
22.	The proposed helpdesk solution must allow IT teams to create solution & make them available on the end – user login window for the most common requests.	
23.	The Helpdesk to be ITIL certified for 10 processes. The helpdesk to have change management along with IPAM, DHCP and DNS management inbuilt in the system.	
ix. Network Monitoring		
1.	Real-time monitoring in production environment for system components on cloud and on-premises	
2.	Should be easy plug and play and enable integration with a wide variety of systems through easy API integration	
3.	Should be able to provide a common dashboard with the required configurable alerts	
4.	Ability to process fifteen thousand flow per second or more per second	
5.	The license should be provided for 400 devices	

### 7.3.20 Asset Management Software (AMS)

Sr. No.	Specifications of Asset Management Software (AMS)	Compliance (Y / N)
1.	Asset Management Solution shall be defined as scalable Web based solution with integrated Configuration Management Database (CMDB) which shall be responsible for management of all IT Assets	
2.	All the required modules either should be from same OEM or should be tightly integrated for single pane of glass view of enterprise monitoring.	
3.	Management of the IT Assets shall include the following: Asset Discovery, Asset Onboarding, Asset Tagging, Asset Inventory, Contract Management, License Management, Life Cycle Management, Reporting Services.	
4.	Solution should be able to identify the IT Assets inside the network through Agent Based and Agent Less discovery techniques along with the functionality of distributed scan/discovery	
5.	Manual Onboarding: For IT and Non-IT Assets not connected to the network, Solution shall allow for manual onboarding of the Assets. Manual onboarding shall be done through either or through a combination of the below: 1) Upload of Asset data files (csv) into the solution. 2) Upload of Asset data through manual entry.	
6.	For proper management of the IT Assets, each asset must be tagged to a user /owner for which Asset Tagging capability should be available in the system.	
7.	The solution should support tagging of assets with Barcode as well as QR code	

8.	IT inventory should include all the details of hardware such as Vendor, Serial Number, Chip Set, CPU information, RAM, numbers of CPUs & Cores, Detail information on Network devices, internal & peripheral disk drives, BIOS details, IP/MAC addresses, End Point/Device name, End Point/Device model, Hard Disk, Storage Devices details, all application and software including in house developed applications / programs, virtualized applications, OS versions and Service Pack information, etc.	
9.	Contract Creation for all onboarded IT Assets. Contract Creation maybe at the time of onboarding or at a later date.	
10.	Contract Creation may include upload of details & documents of Service Level Agreement	
11.	Contract tracking by providing alerts and triggers regarding completion of contracts/renewals due.	
12.	The solution shall provide for life cycle management for both hardware and software assets. The solution shall track the life cycle through Purchase, In production, Renewals, End of Life and Disposal stages of the IT Assets. Solution shall provide alerts for each stage of any such IT Asset.	
13.	The solution should support integrated login portal and single user interface for the solution users.	
14.	The solution should maintain an up-to-date inventory of distributed hardware and software assets.	
15.	The Solution should have capability for discovery of IP based end-user computing devices based on range of IP addresses or IP subnets	
16.	The solution should provide a powerful reporting engine that enables administrators to schedule large batch reports, which can be automatically e-mailed to multiple recipients. Reports can be created in multiple formats such as PDF, CSV, word, and excel, and revisions of past report output can be archived	
17.	The solution must have built-in support for encrypted communications between components without requiring additional software/hardware.	
18.	The Proposed solution should support Software License Metering: Helps to understand the software license compliance and the use of unauthorized software in the organization and helps to act proactively to curb illegal usage and problems associated with it.	
19.	Solution must include a software catalog that identifies All commonly used applications/thousands of Standard publishers/software vendors & their solutions.	
20.	The Solution should provide history capability till each asset level for hardware/software changes for troubleshooting/auditing purposes	
21.	The Solution Should provide Scheduler to determine when the inventory scans can be scheduled for specific group of devices at pre-defined intervals.	
22.	The solution should have capability to discover all unmanaged IP based devices like desktops, servers, laptops, printers, switches, and routers.	
23.	The solution should have ability to track changes in inventory details.	
24.	The solution should have full inventory scan for newly discovered devices for all hardware and software. All subsequent scans should be delta scan only	
25.	The solution should have the ability to identify and maintain records of virtual hosts	

26.	The solution should have auditing capabilities for remote control sessions done using inventory management solutions	
27.	The proposed solution must provide asset baselining to manage and track asset effectively.	
28.	The System should be able to do Inventory governance, including software (authorized and unauthorized) and hardware components.	
29.	The System should be able to report last logged in user for any particular asset.	
30.	All hardware asset information shall be recorded in the management server and some of the basic information shall include but not limited to i. CPU speed and type, ii. Hard disk space, iii. Computer name, iv. Computer model, v. IP address, vi. Operating System vii. Attached peripherals	
31.	The Solution should be capable to support each local admin to maintain cost & depreciation sheets with respect to each asset/at Aggregate level within ASSET Management Tool itself.	
32.	Solution must have the ability to import contract information like PO, AMC Contract etc. from an external source like Excel/CSV file & link with specific Assets.	
33.	The solution should also support tracking of warranty/AMC information of covered endpoints and raise expiration alerts	
34.	The Solution should operate without requiring the devices to belong to a Domain or Active Directory. The Solution shall be capable of integrating with one or more Active Directory structures if present; but should not require the schema to be extended.	
35.	The Agent should be able to coexist with other end point clients like antivirus, DLP, Application whitelisting Solutions etc	
36.	The Information reported should not be more than 1 day old for devices that are active on the network.	
37.	The Solution should have ability to create multiple reports within the dashboard	
38.	The Access to reporting function should be controlled based on rights assigned by the Master Administrator.	
39.	The Solution should allow console operators to create and save graphical reports (e.g., pie, bar, line charts)	
40.	The Solution should allow console operators to customize and save the reports without the use of third-party reporting tools	
41.	The Solution should allow console operators to drill-down from the report to the specific computers.	

#### 7.3.21 Operating System

Sr. No.	Specifications of operating System	Compliance (Yes / No)
1.	Operating System – Microsoft Windows Server 2022 or latest 64 Bit	

#### 7.3.22 Virtualization Software

Sl. No.	Specification for Virtualization Software	Compliance (Yes / No)
---------	-------------------------------------------	-----------------------

1	Enterprise server virtualization features.	
2	Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another e.g.: FC, NFS, iSCSI, DAS.	
3	Must be compatible with all standard guest OSs (in particular: Windows Server 2012, Windows Server 2016, Windows 10, Windows 8, RHEL, CentOS, Ubuntu)	
4	Virtualization software must have the capability to create virtual machine templates to provision new servers	
5	Must provide minimal downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure	
6	Must enable configuration of virtual machines for 1 node or 2 nodes failure	
7	Must have virtual machine High Availability	
8	Support boot from iSCSI, FCoE, and Fibre Channel SAN. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing, and disk array solutions.	
9	Solution should provide Kubernetes in the control plane of hypervisor for unified control of compute, network and storage resources to run both containers/native pods and virtual machines on the same platform	
10	Must provide intelligent virtual machine placement and initial VM placement in a cluster and distribution of VMs across nodes in a cluster.	
11	Must provide live migration of running virtual machines from one node to another with zero downtime and continuous service availability	
12	In the event of node failure, virtual machines should automatically move and run on other designated node(s).	
13	Hypervisor should provide the ability to hot add CPU, memory, disks and NICs on the fly without any service/VM disruption.	
14	Must have virtual machine automated resource scheduling and auto load balancing of resources across nodes and VMs	
15	Must provide for creation and restore of snapshots for individual virtual machines.	
16	Must allow taking clones of individual virtual machines and have an integrated	

**a. Delivery & Installation:**

- i. The delivery and installation site is, at MRSAC, Nagpur. Delays in delivery/installation will attract levy of liquidated damages as per MRSAC rules.
- ii. The bidder/system integrator (SI) and OEM should undertake full responsibility of delivery, installation & integration of the system.
- iii. System Integrator shall be responsible for Supply, Installation, Testing, Commissioning, Operation and Maintenance of the IT Infrastructure components such as Servers, Data Security components, Storage, Software, and other IT components listed in this RFP, required to be set up in MRSAC. This location shall be treated as On-Premises Data Center (DC) for the project.
- iv. The respective OEM engineers must actively participate in the installation along with the system integrator, for which necessary back-to-back arrangements are to be ensured by the bidder
- v. At the time of installation of the system, if it is found that some additional hardware/software items are



required to complete the configuration, which were not included in the bidder's original list of deliverables, and then the bidder is required to supply such items to ensure the completeness at no extra cost to MRSAC. Vendor should ensure completeness of the list of deliverables in the offer to avoid such discovery during installation

- vi. The bidder may carry out site visit examine any of the MRSAC Server room at a time to be agreed with MRSAC and obtain all information on the existing landscape for assessment of the project that may be necessary for preparing the Bid document.
- vii. Data & Network Security Implementation & Maintenance: Maintenance of existing 170 Licenses of Broadcom Symantec End Point Protection/14 qty. Trend Micro Deep security/Quick heal. In case the MRSAC procures additional antivirus suite licenses, bidder has to maintain the same for 5 years. The bidder is required to maintain these licenses for 5 (five) years or till the validity of the contract.
- viii. System Integrator shall provide a Bill of Material/Bill of Quantity that specifies all the hardware, software and any additional networking components of solution required to be installed in DC and DR to facilitate sizing of common Data Center infrastructure such as Racks, Power, UPS, Cooling and Bandwidth among other components.
- ix. System Integrator shall procure and deploy Central Monitoring software, etc. that monitors/manages the entire application, infrastructure and security related components as described in this RFP. The System Integrator will be required to monitor the service level agreement defined in RFP through the monitoring tools (like Central Monitoring software). The selected System Integrator will ensure that the reports for monitoring of most of the SLAs like system uptime, connectivity uptime, performance of servers etc. are generated automatically from the system and calculation of applicable penalties as indicated in the RFP.
- x. These tools shall be transferred to the MRSAC at the completion of the contract. The Department retains the option to have the tools deployed by the System Integrator audited itself or by any of its nominated agencies. The Department also reserves the right to procure and deploy its own SLA monitoring tool for monitoring of SLAs during contract. In such a case, the System Integrator will be required to support the deployment and operation of these tools during the project.
- xi. The System Integrator shall also deploy a backup software to periodically backup relevant data and software. Backup rules and configurations must be detailed by the bidder in the technical proposal.
- xii. The System Integrator is required to furnish a detailed BOM of the Hardware and software requirements. Suggestive hardware & software specifications are mentioned in this RFP.
- xiii. **Note:** The System Integrator will ensure that all the licenses of proposed application/system software & hardware, etc. procured for this project are procured in the name of MRSAC. Sizing of non-IT components required to support the IT components (supplied by bidder as part of this RFP) must be submitted by the bidders in their technical proposal.
- xiv. Bidder should supply, install test & commission the systems as per the configuration at MRSAC On-Premise's site in Nagpur. System supply, installation, testing, commissioning is the responsibility of the bidder and OEM. The bidder must ensure, the respective OEM participation for the installation of storage, servers, file system solution and WAN/internet equipment being procured for this requirement.
- xv. The scope of the installation covers the complete installation, testing and commissioning of all the hardware and software items offered as part this tender. The scope includes the installation, configuration and testing of the client licenses also. The scope also includes the supply, installation and testing of the cabling and realization of the storage network and external network at the MRSAC. The scope shall also include the configuration of the backup policies. It is the responsibility of OEM to resolve any performance related issues.

- xvi. Bidder should resolve all issues related to compatibility of hardware, drivers, and other system software with Windows/RedHat. In case any subsystem requires power, sourcing which is different from the standard options, bidder shall indicate the power requirement for such subsystems clearly. Bidder shall provide site-planning guide for all the subsystems quoted. The bidder must provide ATP documents for the storage and network solutions as part of this tender. The bidder should clearly provide escalation matrix for resolving problems.
- xvii. Minimum 17 nos. of VMs to be created for Cluster-1 (Development), 37nos. VMs to be created for Cluster-2 (Staging), 11 VMs to be created for Cluster-3 (Maintenance) for GIS Applications (ESRI applications- ArcGIS & Hexagon applications- Apollo server, Non ESRI applications, Open-source applications + testing).
- xviii. Mutually acceptable Acceptance Test Procedure (ATP) document should be provided by the vendor. ATP will be conducted on the supplied system

#### **b. Technical Terms & conditions**

- i. The vendor must be a reputed system integrator & authorized partner of the OEM and provide authorization certificates from all OEMs specific to this enquiry must be submitted.
- ii. The brand & models of all the quoted items must be clearly specified. Technical literature/brochure/data sheet in support of the offered solution/products must be enclosed
- iii. In the technical bid, the list of deliverables/Bill of Material (BoM) with Part Nos. as applicable must be clearly specified.
- iv. Unpriced commercial bid (template without prices) must also be submitted in the technical bid
- v. Any item given as complied but not listed in BoM is liable to be treated as non-compliant
- vi. Near obsolete and outdated technology-based products must not be quoted/offered as a part of the solution.
- vii. All supplied items must be brand new and refurbished items are not acceptable
- viii. Each item offered shall have a minimum support life of seven years.
- ix. The system integrator must have similar experience in installation/maintenance of HCI solutions with documentary proofs enclosed
- x. The vendor must have skilled, OEM trained and experienced manpower with technical competence in Nagpur on the quoted products to provide comprehensive warranty with onsite visits as required.
- xi. The bidders should submit the benchmark results along with the technical bid, additionally a Factory Acceptance Test (FAT) should also be carried out to ensure bidders do a proper groundwork before quoting.
- xii. The Bidder shall demonstrate all the performance figures stated in this section during Factory Acceptance Tests (FAT), which will be conducted before the shipment of the items to MRSAC.
- xiii. The selected bidder shall conduct Factory Acceptance Test (FAT) to demonstrate the performance results namely IOPS, random read performance IOPS, creates/deletes, etc. as specified in this RFP for all storage systems. Bidders may please note that FAT is mandatory and not negotiable. Same (or better) performance figures must be demonstrated during ATP at MRSAC.
- xiv. Supplied items should work on AC/230V. All power sockets/fixtures at the installation site are Indian

type

- xv. If the system requires power sourcing that is different from the standard, vendor shall indicate the same and provide the necessary adapters
- xvi. The quote must be complete in all respects. Incomplete and ambiguous quotes are liable to be rejected
- xvii. Amendments/additions to tender after opening of bids are liable to be ignored.

**c. Warranty & Technical Support:**

- i. All the quoted hardware's/software's will have comprehensive onsite warranty support of 05 years with (24hrs x 7days) back-to-back support from OEM, 6 hours response and NBD parts replacement/resolution time. The comprehensive on-site warranty shall start from date of successful completion of ATP.
- ii. The bidder must have necessary back-to-back arrangement with the OEM to ensure competent and timely support
- iii. Failure to maintain the stipulated response/resolution times and an uptime of 99% every quarter will result in levy of penalty charges of 0.1% of total order value per day without any upper limit
- iv. The warranty shall include all hardware and software including hard disks, batteries, SSD drives/devices etc. and supply & installation of updates and upgrades of the software including firmware, OS storage resource management software, etc.
- v. Failed disks must be replaced with new ones at no extra charges and the faulty disks will not be returned to the vendor as per MRSAC rules. No disk retention charges would be paid.
- vi. The technical support from vendor includes reconfigurations, performance optimizations, guidance on usage and software aspects, technical help in planning for augmentations, etc.
- vii. The vendor must have relevant OEM trained certified engineers locally available in Nagpur to provide warranty support
- viii. The vendor should provide escalation matrix for resolving problems
- ix. All supplied software & firmware licenses must be perpetual, upgrades & updates must be provided during the entire warranty period
- x. None of the products quoted should be in the end-of-life list applicable for the next 5 years as announced by the respective OEMs
- xi. System Integrator/bidder must warrant all hardware equipment, accessories, spare parts, software etc. procured and implemented as per this tender document against any manufacturing defects during the comprehensive warranty period.

**d. Post Warranty Maintenance Support:**

- i. The vendor must mandatorily quote for the post-warranty on-site comprehensive annual maintenance contract (AMC) charges for the next 2 years after initial five (05) year warranty Period is Completed.
- ii. The AMC terms are same as those for warranty support and include all software's/firmware updates, upgrades & technical support.
- iii. The 2-year post-warranty AMC (after the initial warranty expires) charges will be paid at the end of each quarter on satisfactory services.

**e. Ownership of the provided accessories.**

- i. Total Hardware and Software accessories shall be owned by MRSAC, and bidder should submit valid copies of licenses to MRSAC before receiving payment. Bidder shall maintain/upkeep the hardware & software for 5 years from the date of Go-Live/Commissioning.
- ii. MRSAC may procure (at its own cost) and add additional hardware & software compatible with existing system, up to a maximum limit of 25%. The bidder must maintain the additional hardware and software without any extra cost to MRSAC, i.e., at the same price as quoted in the commercial bid. Free delivery at site including loading and unloading. Delivery as per the working time of the buying organization (9:45AM to 6:30PM).

**f. Other Terms & conditions:**

- i. MRSAC already has email service from NIC. Bidder must provide necessary support for integration of such email service with the active directory implementation in MRSAC.
- ii. There should be single point of contact from bidder for Solution level support for all the products and solutions required in the BoQ along with technical support for which are not listed above. Resident Engineer at MRSAC site for the period of 5 years for all supplied technologies in three shifts (24 x 7 x 365), minimum three engineers in each shift (System engineer, Network, and Cyber security Engineer).
- iii. Warranty period will be of min 5 years, Global 24 x 7 Product level support, 24-Hour Access to Online resources, Network Management/Operating System/Software updates and upgrades, Proactive diagnostics and immediate alert on the devices, Web based user community for self-service support, Primary point of contact with solution level expertise, Accountability for issues resolution, no matter where it resides, Coordination between various vendors which are part of the solution to resolve the issue.
- iv. 8 x 5 next business day support for 5 years with 24 hours web, telephonic, email technical support assistance.
- v. The vendor must conform to the requirements of security deposit, performance bank guarantee and other terms as specified in the general tender terms
- vi. The vendor shall provide technical compliance for all the tender specifications clauses above. The compliance matrix shall cover all clauses in all sections in the tender specs including 'Delivery & installation', 'Warranty & technical support', and 'other technical terms and conditions'

**g. Capacity Building and Training**

System Integrator/bidder shall be responsible for imparting trainings (on usage, management & monitoring the hardware & software procured through this RFP) to five (5 nos.) office staff members nominated by MRSAC. The training will be imparted once (before project go-live) and shall be scheduled by bidder (in consultation with MRSAC) in a way that information related to each hardware & software is covered. High level responsibilities of bidder for capacity building and training are as follows:

- i. Develop Overall Training Plan
- ii. Develop Training Schedule and Curriculum
- iii. Develop Training Material (five hard copies and one soft copy)
- iv. Deliver Training to Users along with certification by bidder and OEM

Training on IT infrastructure (HCI, Security, Network) Usage, Management & Monitoring.

#### **h. Site Engineers (Project Personnel)**

The successful SI/bidder shall provide site engineers for Server, Network and Cyber security monitoring and support on 24 x 7 and 3 shifts basis at MRSAC, Nagpur for five (05) years. MRSAC shall provide seating space for project personnel.

This manpower shall be responsible for (but not limited to):

- i. Server configuration, OS Patch management, Server monitoring & maintenance, Active Directory implementation and maintenance
- ii. Shutdown/startup of servers, shut down/start up by remote terminal
- iii. Providing access to servers by authorized user accounts
- iv. Monitor & maintain network, HCI, Firewall, server HDD status, HDD failure SAN HDD, NAS Status for its healthiness, monitor firewall working status, network status
- v. Monitor server application web services running status
- vi. Report/escalate to Project Manager in case of failure for attending the problem, attending web services related problems in IIS & Apache TOMCAT servers, for security maintain the server room access logs, server log reports as may be required by MRSAC from time to time.
- vii. Creation and management of server virtualization and desktop virtualization.
- viii. Monitor AC-Cooling status logs,
- ix. Attending and resolving Networking and Cyber security problems including but not limited to lease line status, switch, router, I/O, cable, connectivity problems.
- x. Relocation of IT hardware and software in case of the On-Premise's infrastructure is shifted to new location and providing services at new location.
- xi. Exposure to ISO 27001/ISO20000 preferred for the deployed site engineers.
- xii. One project manager, three network engineers, three system specialists, three Cyber security specialists and one systems specialist in three shifts (each of 8 hrs.) should be positioned by the selected SI/bidder in the site during warranty period on 24Hrs x 7Days basis. Manpower charges will be paid to the bidder on quarterly basis.
- xiii. The bidder should quote the cost per person per specialty per annum.
- xiv. The successful SI/bidder shall appoint Project Manager who will be the single point of contact (from the date of signing of contract) and shall be available for discussions & meetings whenever required by the MRSAC. Project Manager shall be deployed at onsite from the date of project go-live on 8 hours, 1 shift basis (during working days of MRSAC; unless there is an emergency when the Project Manager should be available) for 5 years of post-implementation. The bidder should also appoint suitable number of resources (System, Network, Cyber Security) for Infrastructure deployment & support during deployment and Operations & Maintenance phase. The minimum qualification & relevant experience of the project personnel is given below:

*Table 8 Project Personnel*

S.N.	Proposed Resource	Qty	Academic Qualification	Relevant Experience
1.	Project Manager	1	<ul style="list-style-type: none"> <li>• BE/B. Tech/MCA or equivalent</li> <li>• MBA preferred</li> <li>• PMP, PRINCE2, AGILE certification or equivalent preferred</li> </ul>	<ul style="list-style-type: none"> <li>• &gt;=8 years of total experience including 5 years of project management experience of large Enterprise IT Projects.</li> <li>• Should have undertaken the ownership of organization wide initiatives such as capacity building, business process re- engineering, training etc.</li> <li>• Experience of managing cross- functional teams of minimum 5 to 10 people</li> <li>• Experience in government/public sector is preferred</li> <li>• Should understand IT infrastructure deployment in DC &amp; DR.</li> <li>• He should be able to manage the entire team and project operations. He is required to submit the monthly reports/status to the Director at MRSAC.</li> </ul>
2.	Systems Engineer	1	<ul style="list-style-type: none"> <li>• BE/B. Tech/MCA or equivalent</li> <li>• MCSE/MCSD/MCSA or equivalent certification preferred</li> </ul>	<ul style="list-style-type: none"> <li>• Members should have minimum 4 years of experience in IT Infrastructure implementation and security</li> <li>• Should have experience in hardware &amp; system software installation in DC/DR</li> <li>• The system engineers should have hands-on experience on servers, storage, backup, operation of application software's, HCI, cloud services management etc.</li> <li>• Should be able to identify performance, reliability, security &amp; integration bottlenecks and suggest improvements</li> <li>• They are required to work under the supervision/guidance of the above project manager</li> </ul>

3.	Network Engineer	1	<ul style="list-style-type: none"> <li>• B. Tech/BE/MCA</li> <li>• Relevant Certification (CCNP/CCNA/ACE-A/JNCIA/ADCNS/ASTA/ACSS or equivalent)</li> </ul>	<ul style="list-style-type: none"> <li>• Members should have minimum 4 years of experience in IT network implementation and security</li> <li>• Experience in installation of Network components- both active &amp; passive (routers, core switches, TOR Switches, managed access switches etc.)</li> <li>• Should have experience in identifying network threats and suggesting remedies</li> <li>• Should be able to identify performance, reliability, security &amp; integration bottlenecks and suggest improvements</li> <li>• The network engineers should have hands-on experience on network devices such as router, switches, load balancers, HCI, firewall, internet usage, cloud services management etc.</li> <li>• They are required to work under the supervision/guidance of the above project manager</li> </ul>
4	Cyber Security Engineer	1	<ul style="list-style-type: none"> <li>• BE/B. Tech/MCA or equivalent</li> <li>• Cyber Security certification preferred</li> </ul>	<ul style="list-style-type: none"> <li>• Members should have minimum 4 years of experience in IT network implementation and security</li> <li>• Experience in installation of Network components- both active &amp; passive (routers, core switches, TOR Switches, managed access switches etc.)</li> <li>• Should have experience in identifying network threats and suggesting remedies</li> <li>• Should be able to identify performance, reliability, security &amp; integration bottlenecks and suggest improvements</li> <li>• The cyber security engineers should have hands-on experience on devices such as WAF, firewall, VAPT operation, IPS, IDS, PIM-PAM, HIPS, DLP, End point APT, SIEM, NAC, NMS, EMS, Asset Monitoring, Web proxy etc.</li> <li>• They are required to work under the supervision/guidance of the above project manager</li> </ul>

#### i. Setting up Help Desk Services

- i. System Integrator/bidder shall be responsible for providing support to MRSAC officials in operating the IT Infrastructure (systems, network, Cyber security) and provide remedy for the errors/faults as per the defined SLA's. Helpdesk should be available 24 x 7 and 3 shifts basis at MRSAC, Nagpur. Helpdesk would be responsible for any infrastructure, network, and security issues. SI/bidder must provide a ticketing

management solution for maintaining logs of calls from users, tickets opened, tickets closed and further reporting of response and resolution time as part of SLA monitoring.

- ii. The help desk services should include email and on call support. System Integrator/bidder shall set up help desk services for logging of issues/incidents related to failure of application and infrastructure components and shall provide resolution as per the SLA defined in Section 9. SI/bidder must provide a ticketing management solution for logging calls and conforming to SLAs.

#### **j. Testing**

The System Integrator/bidder shall conduct Onsite Acceptance Test (OSAT). The System Integrator/bidder shall obtain the approval certificate from MRSAC on testing approach and plan. The System Integrator/bidder shall perform the testing of IT infrastructure based on the approved test plan, document the results, and shall fix the bugs/gaps found during the testing. System Integrator/bidder shall share test results along with the screenshots with MRSAC.

It is the responsibility of the System Integrator/bidder to ensure that the end product delivered meets all the requirements of the MRSAC as specified in this tender document.

Following is the list of activities (not exhaustive) to be carried out by the System Integrator/bidder testing:

- i. Test procedures covering all scope of deliverables shall be submitted by System Integrator/bidder prior in the form of Acceptance Test Plan (ATP) document
- ii. System Integrator/bidder shall perform testing, as per approved ATP document
- iii. System Integrator/bidder shall conduct the Stress test using suitable tools in accordance with the approved test plan
- iv. System Integrator/bidder shall perform onsite acceptance testing (OSAT) in the presence of by the identified employees of MRSAC, who are responsible for day-to-day operations. The System Integrator/bidder shall share the test cases and demonstrate the testing procedure to the identified employees of MRSAC.

The System Integrator/bidder shall fix the bugs/errors found during the OSAT, if any, document the results of the testing and submit a report to the MRSAC.

Clearance certificate will be issued only after successful completion of OSAT. No tolerance is permitted at OSAT stage for partial clearances of tests. If the System Integrator does not pass OSAT, a retest shall be conducted with a penalty of 10% of contract value. The retest must be conducted within 4 weeks from first OSAT start date. The contract will be forfeited, if the System Integrator/bidder is unable to fix bugs/errors in the given timeline or is unable to pass the retest.

#### **k. Product Documentation**

- i. The System Integrator/bidder will provide detailed system documentation for reference of MRSAC. System Integrator/bidder shall submit user manual for all IT infrastructure components incorporating all technical intricacies and functionalities provided by the systems. MRSAC expects the following (not limited to) in the form of product documents.
- ii. Configuration Documentation: Consisting of System configuration parameters for each tool deployed.



- iii. User manual including system instructions and use cases, running of a program to perform specific task in the system with sample reports, screen formats, data dictionary, details of menus & instructions on how to perform specific tasks in the system via help of screen shots etc.
- iv. Any other documentation required for usage and maintenance of IT Infrastructure like Equipment Manual, Installation Manual, User Manual & Operational Manual for all supplied hardware & software.
- v. Documentation on Data Centre, Network & Cyber Security Architecture, Database Architecture, All Test Plans for System Testing, Stress Testing, OSAT etc., Requirements Traceability Matrix, Capacity Building Plan & Training Material, SLA and Performance Monitoring Plan, Knowledge Transfer Plans, Issue Logs.

## **1. System Monitoring & Compliance to SLA**

### **a. Up time and performance requirements**

The System Integrator/bidder shall ensure compliance to up time and performance requirements as indicated in this RFP. System Integrator/bidder shall also be responsible for below mentioned activities:

- i. Project Management and Review.
- ii. Logging, tracking and resolution of issues
- iii. Monitoring of system software and tools deployed to ensure that they function reliably.
- iv. Monitor components, including but not limited to, Application servers, Database Servers, and Middleware on an ongoing basis to ensure smooth functioning of the applications.
- v. Maintain Configuration Information & System documentation
- vi. The System Integrator/bidder shall maintain and update documentation of the IT Infrastructure to ensure that:
- vii. Software and Hardware documentation is updated to reflect on-going maintenance, in accordance with the defined requirement.
- viii. User manuals & training manuals are updated to reflect on-going changes/enhancements
- ix. Standard practices are adopted and followed in respect of version control and management of system documentation.
- x. Technical Support Services
- xi. System Integrator/bidder shall maintain data regarding entitlement for hardware & other related software enhancements, replacements, and maintenance.
- xii. If the Operating System or additional copies of Operating System are required to be installed/reinstalled/de-installed, the same should be done as part of same project.
- xiii. Updates/New releases/New versions - The System Integrator/bidder shall provide and implement from time to time the Updates/New releases/New versions of the COTS product, system software and operating systems as required. The System Integrator/bidder should provide updates & patches of the software and tools as and when released by OEM without any cost to MRSAC.
- xiv. System Integrator/bidder shall provide patches to the licensed software, operating system, databases, and other applications.
- xv. Software License Management

The System Integrator/bidder shall provide for software license management and control. System

Integrator/bidder shall provide complete manufacturer's technical support for all the licensed software problems and/or questions, technical guidance, defect, and non-defect related issues. System Integrator/bidder shall provide a single-point-of-contact for software support and provide licensed software support including but not limited to problem tracking, problem source identification, problem impact (severity) determination, bypass and recovery support, problem resolution, and management reporting.

b. Warranty & Annual Maintenance Contract (AMC)

System Integrator/bidder shall provide comprehensive warranty and maintenance services for the software, hardware and other IT infrastructure installed for a period of 5 years from the date of Project Go-live. Post warranty support shall be provided for year-on-year basis as per tender requirements.

- xvi. In case Go-live extends beyond schedule, then warranty for all the tendered items shall also be extended correspondingly by the System Integrator.
- xvii. System Integrator/bidder must warrant all hardware equipment, accessories, spare parts, software etc. procured and implemented as per this tender document against any manufacturing defects during the warranty period. The following key points must be noted by the bidder:
- xviii. The bidder shall quote for year wise comprehensive Annual Maintenance Contract (post warranty) for two years (6th & 7th year) which shall become effective at the end of the 5 years warranty period.
- xix. No separate charges shall be paid for visit of engineers or attending to faults and repairs or supply of spare parts
- xx. During warranty and AMC period, faulty HDD, storage, and magnetic media must be replaced but the same will not be returned for replacement and RMA.
- xxi. During the implementation period and warranty period System Integrator/bidder shall perform all the functions as enunciated in contract at no extra cost to MRSAC. All the penalty clauses shall be applicable during the implementation period and during period of warranty in case of failure on part of bidder
- xxii. The bidder, at the time of submitting the bid, shall submit the proposal specifying the fault control center location and plan to carry out repair under AMC. The bidder shall also indicate what spares will be kept in different locations
- xxiii. If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months or six times in a period of less than twelve months, it shall be replaced by equivalent or higher-level new equipment by the System Integrator/bidder at no cost to MRSAC
- xxiv. The System Integrator/bidder shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for virus, if any, and should maintain proper records for such PM.
- xxv. Failure to carry out such PM will be a breach of warranty, and the warranty period will be extended by the period of delay in PM.
- xxvi. The System Integrator/bidder shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures
- xxvii. System Integrator/bidder shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met
- xxviii. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).
- xxix. The System Integrator/bidder shall develop and maintain a database of IT inventory to include the registered hardware warranties.

- xxx. The System Integrator/bidder shall intimate MRSAC well in advance regarding expiry of warranty period of any hardware and software supplied by bidder or procured by MRSAC (and maintained by bidder).
- xxxi. The warranty shall start from the date of successful completion of ATP.
- xxxii. The bidder should also quote the price for extended warranty for the total solution on annual basis for a period of two more additional years after completion of five years warranty.

**m. Exit Management**

System Integrator/bidder will be responsible for formulating a detailed exit management plan to help facilitate MRSAC in managing the project upon exit of the System Integrator/bidder. The plan should clearly outline the risks involved and give a detailed transition schedule between the two entities. This exit management plan must be submitted to MRSAC within 3 months from the date of signing of contract and will be subject to approval from MRSAC or any of its nominated agencies.

Every six months, department may ask the bidder to share the details of all the assets, SOP, server and software access details, software maintenance details etc. for review and audit by a Third-party auditor. The department might choose to audit the completeness of the plan and/or execute a dry run of this exit management plan.

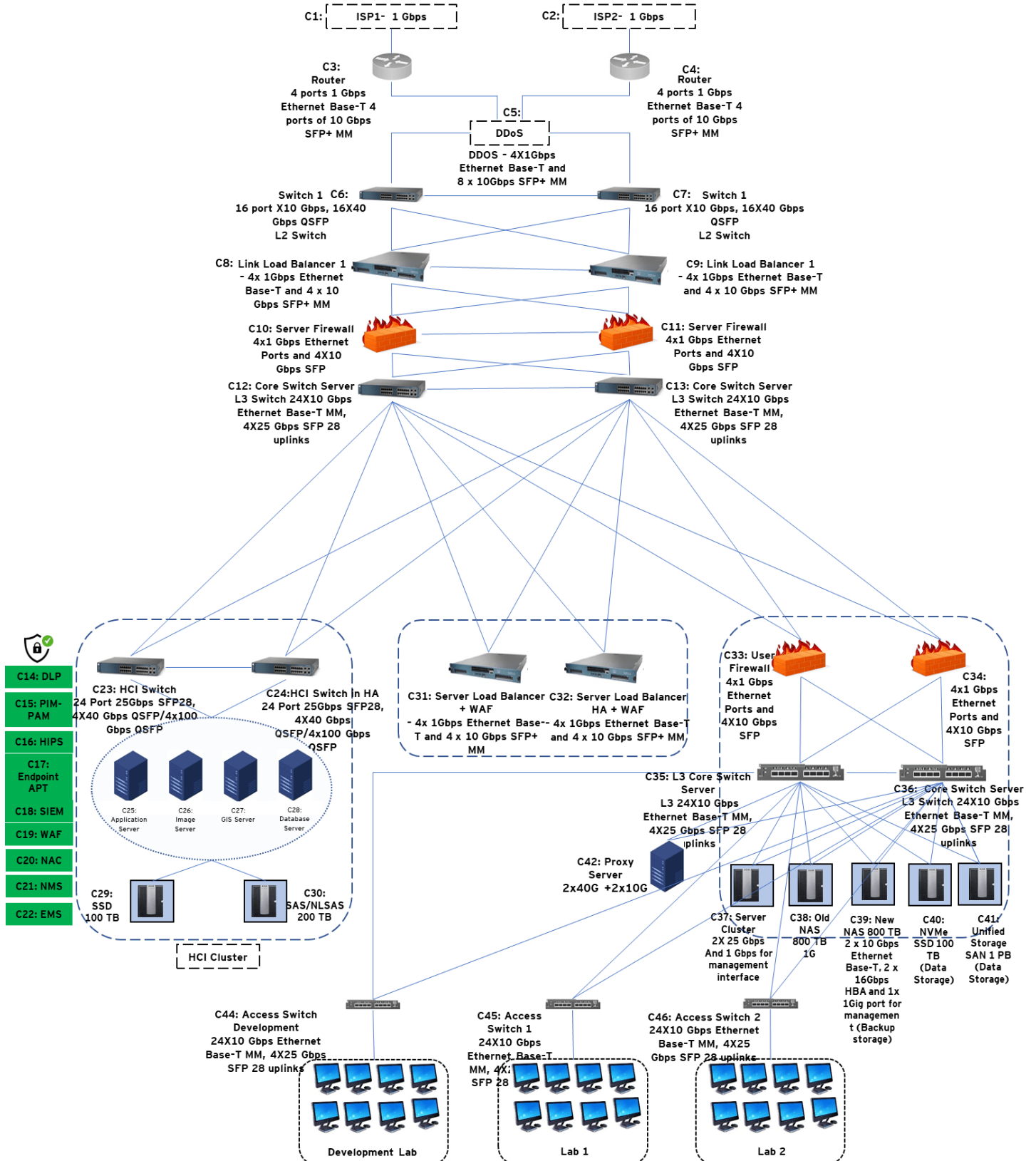
**n. Implementation and adherence to IT policies as defined by MRSAC**

SI must implement and adhere to the IT policies as defined by MRSAC from time to time.

o. System Architecture for On Premise items at MRSAC:

Table 9 System Architecture for On Premise Data Center at MRSAC

## Indicative MRSAC System Architecture - On Premise



## 8 Implementation Plan & Payment Schedule:

### 8.1 Implementation Plan

Implementation of the project will entail infrastructure deployment and OSAT activities for project Go-Live. Project Go-Live is scheduled in 4 months from the time of award of contract. Successful project implementation shall be followed by operations and maintenance support for a period of 5 years. Critical Project Milestones have been given in the subsequent section to provide more clarity on the scope of project.

### 8.2 Project Milestones

Several project milestones have been identified and linked to various activities under the scope of work of System Integrator/bidder. The table below elucidates various milestones and deliverables that need to be submitted by the System Integrator/bidder. MRSAC reserves the right to change/alter list of deliverables at its own discretion.

*Table 10 Project Milestone*

Timeline (in weeks)	Project Milestone	Deliverables	Payment Milestones
T	Signing of Contract	<ul style="list-style-type: none"> <li>Signed Contract</li> <li>Performance Bank Guarantee (10 % of Total Contract value)</li> </ul>	-
T + 2	<ul style="list-style-type: none"> <li>Project Kick Off - Detailed Project Plan</li> <li>Preparation of a Risk Management and Mitigation Plan</li> <li>Preparation of Manpower Deployment Plan</li> </ul>	<ul style="list-style-type: none"> <li>Detailed Project Plan for Implementation of the Project</li> <li>Risk Management and Mitigation Plan</li> <li>Manpower Deployment Plan</li> <li>Detailed plan for monitoring of SLAs and performance of the overall system</li> </ul>	<b>M1:</b> Submission of Detailed Project Plan including risk management, manpower deployment and SLA
<b>Pre-design Phase</b>			
T + 3	<ul style="list-style-type: none"> <li>Site assessment for Infrastructure Deployment</li> </ul>	<ul style="list-style-type: none"> <li>Site Assessment Report</li> </ul>	-
<b>Design Phase</b>			

T + 5	<ul style="list-style-type: none"> <li>Detailed Design: High Level Design (including but not limited to) <ul style="list-style-type: none"> <li>Logical and physical database design</li> </ul> </li> <li>Low Level Design (including but not limited to) <ul style="list-style-type: none"> <li>Data Centre, Network &amp; Security Architecture</li> <li>Database Architecture</li> </ul> </li> <li>Development of test cases (System Testing and OSAT)</li> <li>Final BoM with detailed technical specifications for the IT Hardware &amp; Software, Network, and other IT Infrastructure Requirements</li> <li>Infrastructure Deployment plan based on site assessment and concurrence with MRSAC</li> <li>SLA and Performance Monitoring Plan</li> </ul>	<ul style="list-style-type: none"> <li>Acceptance Test Plan</li> <li>Final BOQ</li> <li>Infrastructure Deployment plan</li> <li>Postimplementation (production) performance and O&amp;M plan</li> </ul>	-
<b>Deployment Phase</b>			
T + 13	<ul style="list-style-type: none"> <li>Delivery of hardware &amp; software</li> </ul>	<ul style="list-style-type: none"> <li>Delivery Receipt</li> <li>Inspection &amp; Acceptance Report</li> <li>Equipment Manual, Installation Manual, User Manual &amp; Operational Manual, System Administration Manual for all supplied hardware &amp; software</li> <li>Toolkit/Troubleshoot guide for software &amp; hardware</li> </ul>	<b>M2:</b> Delivery Receipt and Inspection & Acceptance Report of delivered hardware & software
T + 17	<ul style="list-style-type: none"> <li>IT Infrastructure deployment at site provided by MRSAC</li> <li>Installation &amp; Integration</li> <li>Preparation of training curriculum and training materials</li> <li>Training on IT infrastructure and Network Monitoring(s)</li> <li>Third Party Audit (If conducted by MRSAC or its agency)</li> <li>OSAT &amp; Project Go-live completion report</li> </ul>	<ul style="list-style-type: none"> <li>IT Infrastructure Installation Report</li> <li>Training material</li> <li>OSAT &amp; Project Go-live completion report</li> <li>Training feedback report</li> </ul>	<b>M3:</b> OSAT Completion & Project Go-live Report

Operations & Maintenance (O&M) [Continuous activity for 5 years after Project Go-Live (T+17 to T+260)]	<ul style="list-style-type: none"><li>• Logging, tracking and resolution of issues.</li></ul>	<ul style="list-style-type: none"><li>• Monthly Progress Report on Project including SLA Monitoring Report and Exception Report</li><li>• Details on all the issues logged</li></ul>	<b>M4:</b> Operation & Maintenance (Equal quarterly payments after ProjectGo-Live till Project Completion)
-----------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------

### 8.3 Payment Schedule

*Table 11 Payment Schedule*

SN	Payment Milestones for the implementation Plan	% Payment of Contract	Time Schedule (All time in weeks)
1.	<b>M1:</b> Submission of Detailed Project Plan including risk management, manpower deployment and SLA	10% of Total CAPEX Cost	T+2
2.	<b>M2:</b> Delivery Receipt and Inspection & Acceptance Report of delivered hardware & software	50% of Total CAPEX Cost	T+13
3.	<b>M3:</b> OSAT & Project Go-live completion report	40% of Total CAPEX Cost	T+17
4.	<b>M4:</b> Operation & Maintenance (Equal quarterly payments after Project Go-Live till Project Completion) + Human Resources/Manpower deployed	Actual maintenance cost (Quarterly basis)	T+17 to T+260

- i. All payments to the system integrator/bidder shall be made upon submission of invoices along with relevant signoffs from MRSAC and only after the acceptance of relevant deliverable(s) by MRSAC.
- ii. For details of Milestones please refer to 'Implementation Plan'.
- iii. Go-Live requires completion and acceptance of the at least following activities performed by the System Integrator/bidder
  - a. Capacity Building Program covering the targeted personnel
  - b. IT Infrastructure setup (Hardware and Software)
  - c. Delivery and Commissioning of Client-Side Infrastructure
- iv. The TDS as applicable shall be deducted.



## 9 Service Level Agreement

### 9.1 Introduction

The purpose of this section is to define the minimum levels of service expected to be provided by the System Integrator/bidder; define the target levels for those services and the measures for demonstrating performance against those targets.

The primary intent of Penalties is to ensure that the system performs in accordance with the defined service levels. Penalties are not meant to be punitive or, conversely, a vehicle for additional fees. Monthly performance evaluation will be conducted using the agreed reporting periods.

Penalties (in both Implementation Phase and Post-Implementation Phase) against breach of expected service levels shall be collectively deducted subject to a cap of 10% of quarterly payment due to System Integrator/bidder. Department reserves the right to waive off penalty against breach of any of the expected service level considering prevailing circumstances and/or if the reason for breach is beyond the control of System Integrator/bidder.

For purposes of this Service Level Agreement, the definitions and terms as specified along with the following terms shall have the meanings set forth below.

### 9.2 Definitions

- i. Service Name: The type of service that the MRSAC expects the SI to provide
- ii. Service definition: A description of the service and its major components provided by the System Integrator/bidder & MRSAC. The definition includes a broad outline of the service.
- iii. Targeted service level: The standard of service expected in delivery of the described services. This is expressed in terms of scheduled hours of service, availability, reliability, serviceability, and response time, to the extent each term is applicable and relevant to the services unless stated otherwise, as set forth in this document.
- iv. Scheduled hours of service: Scheduled hours of service are defined in terms of the hours within a day, or days within a larger period, during which the system or service should be available. For the purpose of this Service Level Agreement the following definitions are used:
  - Core hours are defined as between 09:45 and 18:15 hours from Monday to Saturday
  - Non-core hours are defined as between 18:15 - 24:00 hours and 00:00 – 09:45 hours from Monday to Saturday, and 00:00 - 24:00 hours on 2<sup>nd</sup> and 4<sup>th</sup> Saturdays, Sundays, and Public Holidays.
- v. Availability: The availability of systems or services is a measure of the length of time the systems or services are available to MRSAC, Nagpur and would be assessed as the proportion of the Scheduled Hours of Service that a service is actually available, measured over each specified period.

Availability means that applications, hardware, and servers for which the SI/bidder is responsible hereunder, are available for use by all user groups. Loss of service availability (an “Outage”) would be deemed to have occurred when the system or a defined component of the system is unavailable.

MRSAC, Nagpur may require services to be available outside Scheduled Hours of Service and at times and for reasons which cannot be specified in advance. To cover this need, the SI/bidder agrees to provide services of short duration outside Scheduled Hours of Service by prior arrangement at mutually agreed times.

Service Availability = (Actual Service Hours Delivered ÷ Scheduled Service Hours) \* 100%.

The actual number of Service Hours delivered by the SI/bidder may be less than the Scheduled number as a result of downtime caused, for example, by the failure of hardware, the failure of application software or unscheduled maintenance. The total application system downtime experienced by MRSAC, Nagpur during a period is the number of Service Hours lost by the site as a result of outages.

The actual level of service delivered is calculated by subtracting the Total Downtime (the number of Service Hours lost as a result of downtime/application server unavailability) from the Scheduled number of Service Hours.

Actual Service Hours Delivered = Scheduled Service Hours (-) Total Downtime

The SI/bidder will measure Service Availability, and data regarding system downtime will be collected automatically by the system integrator.

Service Availability will be reported on a regular basis. The figures for actual and planned service hours will then be aggregated to calculate service availability over longer periods and to allow a rolling average to be calculated. Calculated service availability statistics will be used as inputs to Quarterly Service Review Meetings between the MRSAC, Nagpur and the SI/bidder.

- vi. Scheduled Downtime: Time agreed between MRSAC, Nagpur and the SI/bidder during which the system may be made purposefully unavailable to users to enable maintenance to be performed. The maximum scheduled downtime for preventive maintenance allowed is 2 hours (1:00 am to 3:00 am on Sundays) each month. The SI/bidder should notify 7 days in advance of the scheduled downtime or else it will not be classified as scheduled downtime.
- vii. Downtime: The time period for which the specified services/components are not available to MRSAC, Nagpur and excludes the scheduled downtime planned in advance.
- viii. Reliability: The reliability expected from the system or service. The system would provide an acceptable level of reliability in terms of the following:
  - Number of outages, the acceptable level being defined in the Performance Metrics
  - Successful completion of processing, the acceptable level being as specified in the service levels

- ix. Service ability: Service ability outlines the degree to which MRSAC, Nagpur will accept loss of service. Outages measure the time lost per failure. An outage is also defined in terms of the transactions or services that are unavailable, and by the number of users affected. Any incident that meets one or more of the criteria on the list is considered an outage. Each outage would be counted on an incremental basis, regardless of if the same problem recurs several times, unless otherwise agreed. The help desk would be notified of any interruption to the service. If multiple users experience the same problem simultaneously, this will be counted once. Each service level defines a number of 'acceptable' outages in one month and details of these are included in each service level.
- x. Incident: Any event/abnormality in the functioning of an equipment or while providing a service that might lead to disruption in normal operations is termed as an incident.
- xi. Problem Severity: Severity is determined by the scope or impact of the problem. Assignment of severity ratings by the SI/bidder will be on the basis of the best possible assessment of the problem by the SI/bidder.
- xii. Escalation Process: The severity ratings defined in the table below correspond to the basic level of service required by MRSAC, Nagpur. These definitions may not be appropriate in certain circumstances where a problem has the potential to cause MRSAC, Nagpur significant damage to its business or reputation and in such cases a higher severity rating may be requested and authorized by the project management team and negotiated and agreed with the SI/bidder. Alternatively, MRSAC, Nagpur may negotiate with the SI/bidder for provision of a dedicated problem resolution support service on stand-by, either during or outside core business hours, for a limited period.
- xiii. Response Time: The response time is defined as the time taken by the SI/bidder to confirm to the person that originated the call, either by phone or e-mail that the problem is being attended to.
- xiv. Resolution Time: The time taken (after the incident has been reported at the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level or to respective Vendors, getting the confirmatory details about the same from the vendor and conveying the same to the end user), the services related troubles during the first level escalation.
- xv. Severity 1 Issue:
  - a. Service has completely failed or a major failure of any system/Server/Network Component at core or distribution layer making unavailability of critical applications and services which is completely down with critical business impact or degraded with most of the users from various locations.
  - b. Total loss of service to entire user set which includes total unavailability of critical applications for entire end users in all locations.
  - c. Network Security breach detected for core components.
- xvi. Severity 2 Issue
  - a. A key component of solution/network, an application across all users, or a set of critical user or network is down, degraded, or unusable leading to performance and degradation of service.

- b. An incident which is not yet Severity 1 issue but might lead to a potential Severity 1 incident.
  - c. Partial users at a majority location are affected having network/internet/application unavailability but not all the users in all locations.
- xvii. Severity 3 Issue
  - a. System/Network/Application is up and running, but the problem causes non-negligible impact at access layers and user endpoints.
  - b. Does not prevent operation of a business-critical applications/system but there is some degradation in performance (Example: The issue affects only some set of users in accessibility or slower connectivity to core services and application at particular access location.)
  - c. Moderate loss of application functionality or performance resulting in multiple users impacted in their normal functions.
- xviii. Severity Issue: Service/network for certain office location is degraded intermittently with minor business impact or brief periods but remains mostly normal.
- xix. Metric: The measure of performance standards for service levels or supporting measures which the computation formula of the measure may depend upon.
- xx. Measurement Period/Reporting Frequency: The period of time over which availability, reliability, serviceability, and response time will be measured and reported.
- xxi. Responsibility for Measurement: The party designated as being responsible for collecting measurement details. In all cases where the System Integrator/bidder is responsible for an activity according to this Service Level Agreement, the System Integrator is also responsible for assessing and reporting its performance in the manner specified elsewhere in this document.
- xxii. Measurement Method: The definition of how the performance of the service is to be measured and/or calculated as set forth in the Performance Metric for the applicable service level. The measurement will be based on the automated report generated from Ticketing Management System (TMS) or Enterprise Management System (EMS) as mentioned in the SLA tables. The TMS/EMS would play a crucial role in monitoring the Service levels and hence will have to be customized accordingly. The System Integrator/bidder must deploy the TMS/EMS tool and develop additional scripts (if required) for capturing the required data for SLA reporting. This tool should generate the SLA monitoring report on a monthly basis unless stated otherwise.
- xxiii. Service Level Violation: If the System Integrator fails to meet the Minimum Service Levels as reported on a Quarterly basis for a particular Service Level for which he is responsible, it would be considered as Service Level violation.
- xxiv. Service Level Reporting: The SI/bidder will submit the Performance Report on a Monthly basis to the MRSAC's projectmanagement team based on the availability & performance measurements carried out by the SI/bidder and will include the summary of all incidents reported and the associated IP performance for that period.

- xxv. Service Level Review Meetings: To coincide with the regular production of information covering the performance of the System Integrator/bidder against target levels of service there would be a monthly meeting between representatives of the System Integrator/bidder and MRSAC's project management team to review the service being provided. The objective of the service level review meeting is to ensure that all relevant information affecting service provision is exchanged. The service level review should not be seen as a substitute or replacement for normal informal dialogue.

Each service level review meeting agenda should include the following items:

- Are view of the service performance against agreed targets in the period since the last meeting
- The status of specific service issues raised or outstanding at the previous meeting
- A review of work-in-progress against long-standing service problems or issues to be resolved
- Any new problems or issues
- Identification of any discernable trends
- Any action points required for the next meeting
- Any longer-term plans required
- Any minor changes required to the services, service levels or the agreement

### **9.3 Technical Terms and Conditions:**

- i. The SI/bidder should ensure compatibility of the components used in the solution. A letter of confirmation should be attached along with the technical compliance from all the OEMs (Original Equipment Manufacturer) on the interoperability for this tender.
- ii. The SI/bidder shall provide a detailed technical compliance statement for offered products and specifications. The compliance statement is to be prepared in MS-EXCEL format as per the tender sequence and shall use the same serial no for all the items and sub-items as in the tender to be submitted with signed hardcopy without any corrections. The compliance matrix shall also cover all the terms and conditions specified in the tender.
- iii. The SI/bidder should list detailed bill of materials for all the items and subitems offered along with part numbers. Any item given as complied and not listed in bill of material will be treated as not complied.
- iv. The total solution document shall be provided by the SI/bidder along with the technical offer. The SI/bidder should bring out gaps in the tender document, if any, which might be required for completing the total solution and also quote for total solution.
- v. Complete ownership of ensuring the solution in a working condition as per MRSAC requirements mentioned in the tender document lies with the SI/bidder only. Any components/accessories like cables, etc. should be included in the quote and SI/bidder should agree to supply the items missed/short shipped at no additional cost to MRSAC.
- vi. The SI/bidder has to invariably submit MAF for all the items quoted.
- vii. The system integrator must be a tier-one partner of the OEMs and should also provide letter of authorization from the OEMs for this tender. The SI/bidder should participate as a single party and no consortium is

allowed.

- viii. The SI/bidder should not change the OEMs once the tender is submitted.
- ix. Near obsolete and outdated technology-based products should not be quoted/offered as a part of the solution.
- x. Each item offered shall have a minimum support life of seven years.
- xi. One Tera Byte (TB) is equal to 1024x1024x1024x1024 Bytes in this tender.
- xii. The SI/bidder must take full responsibility for total supply, installation, and integration and successful testing of all the quoted items.
- xiii. The SI/bidder must provide item-wise breakup prices, wherever applicable.
- xiv. The quoted make and models must be clearly specified for all the items/sub-items
- xv. Full technical specifications and literature must be provided for all the quoted items including sub-items.
- xvi. The offer must be from reputed principals or authorized primary dealer/system integrator of major principals for these types of products.
- xvii. The SI/bidder must have the proven experience in installing and supporting similar data centers in the last three years in 24x7 working mode. Also, should provide the user/site details with a documentary proof.
- xviii. The SI/bidder must have certified skilled, trained, and experienced manpower with technical competence on all the quoted products.
- xix. Any required software/drivers to make the given items usable should be delivered along with media and documentation.
- xx. All standard and optional items (if any) must be clearly indicated.
- xxi. Licensing information for the quoted software must be provided in detail.
- xxii. The SI/bidder should ensure availability & supply of required spares and consumables at least for the next seven years after installation and successful integration of equipment.
- xxiii. The SI/bidder should be an authorized partner of the OEMs involved in the quotation, for the last three years. The SI/bidder should have implemented the enterprise class storage and networking elements in this period within India.
- xxiv. The OEMs participating in the tender must have presence in India for all their major class of items offered, for at least three years.
- xxv. The SI/bidder should have sufficient experience in doing business with the OEM and should have engineers certified by the OEMs in India.
- xxvi. The SI should have executed large installations in Govt. of India organizations like ISRO, MoES & Atomic Energy.
- xxvii. All Ethernet switches quoted must be from the same OEM.
- xxviii. All necessary cables, connectors, adapters, accessories etc., should be supplied by the SI/bidder as required

for the successful integration of the total solution.

- xxix. Installation, integration, and support have to be performed/provided at MRSAC Campus, located at VNIT Campus, S.A. Road, NAGPUR-10, Maharashtra, India.
- xxx. Mutually acceptable acceptance test procedure (ATP) document should be provided by the SI/bidder. Acceptance Test on the supplied equipment must be conducted as per the ATP document.
- xxxi. Supplied items should work on 230V AC power supply.
- xxxii. While carrying out the structured cabling, any extra cable/connectors used more than the quantities specified; payment would be made at actual.
- xxxiii. All the licenses for given hardware and software should be perpetual and valid for lifelong.
- xxxiv. Any defective/failed storage hard disk or magnetic media (LTO) or any storage media shall be replaced by the SI/bidder on free of cost without insisting on return of defective media during warranty. The defective media will not be given to the SI/bidder.
- xxxv. SI/bidder should provide the total power and Air conditioning requirements along with the quotation for the supplied items.
- xxxvi. SI/bidder should treat all the batteries supplied along with servers/storage systems as components and should replace batteries during warranty period without extra cost.
- xxxvii. All power sockets / fixtures at the installation site are Indian type.
- xxxviii. All the SIs/bidders should provide solution document based on the tender document requirements and architecture given in Figures. For all cabling and deployment references, layout provided may be used.
- xxxix. The SI/bidder shall quote for all the mandatory items and shall ensure that slab rates/unit prices are provided wherever required. No further clarification will be entertained in this regard.
- xl. SIs/bidders are required to upload the unit prices of items specifically sought in this tender or any items the SI feels required to complete the solution, in an encrypted & password protected excel sheet along with the price bid. SIs shall ensure that an unpriced version of this is uploaded along with the technical bid.
- xli. To achieve the active-active site with other distributed nodes, the GSLB (Global Site Load Balancer) functionality in the server load balancer is considered in this RFP.
- xlii. The SIs/bidders who can comply all the above RFP points from 1 to 43 in full should only be participated in the bidding and necessary documentary evidence should be submitted.

## 9.4 Implementation Phase Service Level Agreement (SLA) Criteria with the System Integrator

*Table 12 Implementation phase service level agreement*

Sr. No	Parameter	Metric	Frequency	Penalty	Measurement
1.	Delivery of the reports / deliverables as per the timelines mentioned in the Project Milestones section of this RFP	$\leq 1$ week after the due date	As per Project Milestone	Rs. 5,000 for every week of delay	Dates for delivery of reports
2.	Supply of all hardware and equipment at DC	$\leq 13$ weeks from date of signing of contract	Once	Rs. 10,000 per week of delay	Date of Supply of hardware and equipment at DC
3.	Installation & Commissioning of all hardware and equipment at DC & Go-live of project	$\leq 17$ weeks from date of signing of contract	Once	Rs. 50,000 for every week of delay	Date of Project Go-live

## 9.5 Post-Implementation Phase Service Level Agreement (SLA) Criteria with the System Integrator

*Table 13 post-implementation phase service level agreement*

Sr. No.	Parameter	Metric	Frequency	Penalty	Measurement
1.	Severity 1 Issue	Response Time: $\leq 2$ Hrs. from the time the call is logged by end user.  Resolution Time: $\leq 8$ Hrs. from the time the call is logged by end user.	Daily	1% of quarterly payment per day for the first day, 2% of quarterly payment per day every subsequent day, subject to a maximum of 5.0 % post which MRSAC may invoke Annulment of the contract.	Automated Report as per Ticket Management System.
2.	Severity 2 Issue	Response Time: $\leq 4$ Hrs. from the time the call is logged by end user.  Resolution Time: $\leq 2$ Days from the time the call is logged by end user.	Daily	0.5% of quarterly payment per day for the first day,  1% of quarterly payment per day every subsequent day, subject to a maximum of 5.0	Automated Report as per Ticket Management System.



				% post which MRSAC may invoke Annulment of the contract.	
3.	Severity 3 Issue	Response Time: <= 1 Day from the time the call is logged by end user.	Daily	0.25% of quarterly payment per day for the first day,	Automated Report as per Ticket Management System.
		Resolution Time: <= 5 Days from the time the call is logged by end user.		0.75% of quarterly payment per day every subsequent day, subject to a maximum of 5.0 % post which MRSAC may invoke Annulment of the contract.	
4.	Severity 4 Issue	Response Time: <= 2 Days from the time the call is logged by end user. Resolution Time: <= 10 Days from the time the call is logged by end user.	Daily	0.25% of quarterly payment per day for the first day, 0.5% of quarterly payment per day every subsequent day, subject to a maximum of 5.0 % post which MRSAC may invoke Annulment of the contract.	Automated Report as per Ticket Management System.

Sr. No	Parameter	Metric	Frequency	Penalty	Measurement
1.	Average System Uptime. System Uptime to include: Server/HCI/Unified storage Uptime, Router/Switch/firewall Any other IT component in the Infrastructure architecture (including but not limited to network & security components)	99.90 %	Monthly	2% of quarterly payment for monthly deviations, subject to a maximum of 5.0 % post which MRSAC may invoke Annulment of the contract.	Automated Report as per EMS

Sr. No	Parameter	Metric	Frequency	Penalty	Measurement
1.	Deployment of manpower from the beginning of implementation and post implementation phase	Within 5 days	Monthly	■ Rs.4,000 per working day in case of Project Manager	Attendance

2.	Replacement of existing manpower owing to non-performance upto satisfactory level at the request of Department	Within 30 days from formal intimation. Overlap of old resource to be undertaken for a period of at least 2 weeks.	Monthly	■ Rs.2,000 per working day per human resource in case of other manpower	Attendance
3.	Replacement of selected / existing manpower at the request of the System Integrator /bidder.	Within 30 days from formal intimation. Overlap of old resource to be undertaken for a period of at least 2 weeks.	Monthly		Attendance

## 10 Formats for Pre-Qualification and Technical Bid Submission

### 10.1 Formats for Pre-Qualification Bid Response

SIs/bidders are requested to submit their responses for the Pre-Qualification Requirements clearly labelled according to the following categories.

#### 10.1.1 Details of Organization

(To be submitted on the Letterhead of the responding firm)

*Table 14 organization details*

Details of the Organization	
Name	
Nature of the legal status	
Nature of business in India	
Date of Incorporation	
Date of Commencement of Business	
Address of the Headquarters	
Address of the Registered Office in India	
Other Relevant Information	
Mandatory Supporting Documents:	
a) Certificate of Incorporation from Registrar of Companies (ROC)	
b) Relevant sections of Memorandum of Association of the company or filings to the stock exchanges to indicate the nature of business of the company	

(Signature of the Authorized signatory of the Bidder)

Name:

Designation:

Seal:

Date:

Place:

### 10.1.2 Financial Details

(To be submitted on the Letterhead of the Chartered Accountant)

*Table 15 Financial details*

Financial Information			
	FY 2021-22	FY 2022-23	FY 2023-24
Annual Turnover (in INR crores)			
Average Annual Turnover (in INR crores)			
Net Worth			
Other Relevant Information			
Mandatory Supporting Documents: a) Audit or Certified financial statements for the Last three financial years; (Please include only the sections on P&L, revenue, and the assets, <b>not</b> the entire balancesheet.)			

(Signature of the CA)

Name:

Designation:

Seal:

UDIN:

Membership No.:

Registration No.:

Date:

Place:

Business Address:

### 10.1.3 Previous Project Experience

(To be submitted on the Letterhead of the responding firm)

Respondents must provide details of previous project experience along with mandatory supporting documents, as per the format provided below.

*Table 16 Previous project experience*

Relevant project experience	
General Information	
Name of the project	
Client for which the project was executed	
Name and contact details of the client	
Project Details	
Description of the project	
Scope of services	
Outcomes of the project	
Other Details	
Total cost of the project	
Total cost of the services provided by the respondent	
Place where the project was executed (deployment, operations, and maintenance)	
Duration of the project (no. of months, start date, completion date, current status)	
Other Relevant Information	
Mandatory Supporting Documents: a) Work Orders b) Letter from the client (competent authority) to indicate the successful completion/partial completion of the projects	

(Signature of the Authorized signatory of the Bidder)

Name:

Designation:

Seal:

Date:

Place:

**10.1.4 Format for Declaration by the SI/bidder for not being Blacklisted/Debarred**

(To be submitted on the non-judicial stamp paper of Rs.500/-)

Date: dd/mm/yyyy

To  
The Director,  
MRSAC, Nagpur

Sub: Declaration for not being debarred/black-listed by Central/any State Government department in India as on the date of submission of the bid

Dear Madam,

I/We, the undersigned, herewith declare that my/our company (<-- name of the firm -->) has not been debarred/black-listed by Central/any State Government department in India as on the date of submission of the bid.

Thanking you,

Yours faithfully,

(Signature of the Authorized signatory of the Bidder)

Name:

Designation:

Seal:

Date:

Place:

### **10.1.5 Bid Security Form for EMD**

Whereas\_\_\_\_\_ (hereinafter called "the SI") has submitted its tender offer dated dd/mm/yyyy for providing services for tender "Selection of System Integrator (SI) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project"

KNOW ALL MEN by these presents that we\_\_\_of\_\_\_\_\_(herein after called the Bank) are bound up to (herein after called "the Department ") in the sum of\_\_\_\_\_ for which payment well and truly To be made to the said Purchaser, the Bank bind sit self, its successors and assigns by these presents; sealed with the Common Seal of the Said Bank this\_\_day of\_\_.

THE CONDITIONS of this obligation are:

- If the SI/bidder withdraws its tender during the period of tender validity specified by the Tenderer on the TenderForm; or
- If the SI/bidder, having been notified of the acceptance of its tender by the Department during the period oftender validity:

Fails or refuses to execute the contract Form if required; or

Fails or refuses to furnish the Performance Security, in accordance with the instruction given in tender document.

We undertake to pay the Department up to the above amount upon receipt of its first written demand, without the Department having to substantiate its demand, provided that in its demand the Department will note that the amount claimed by it is due to owing to the occurrence of one or both of the two conditions, specifying the occurred condition orconditions.

This guarantee is valid up to 180 days from last date of bid submission and shall be governed and construed in accordancewith Indian Laws.

Date:

Place:

(Seal of Bank)

(Signature of the Bank Official)

### **10.1.6 Performance Bank Guarantee**

(For a sum of 5% of the total value of the contract)

Ref. No.:

Date :

Bank Guarantee No. :

To

The Director, MRSAC, Nagpur

Against Letter of Intent number\_\_\_\_\_dated\_\_\_\_\_relating to Tender No.\_\_\_for the project

“ \_\_\_\_\_ ” (here in after called the 'LoI') and the contract to be entered into between the MRSAC, Govt of Maharashtra, (herein after called" “) and\_ (hereinafter Called the SI), this is to certify that at the request of the SI we \_\_\_\_Bank, are holding in trust in favor of \_\_\_\_\_, the amount of Rs.\_\_\_\_(Write the sum here in words) to indemnify andkeep indemnified the \_\_\_\_\_ against any loss or damage that maybe caused to or suffered by the \_\_\_\_\_ by reason of any breach by the SI of any of the terms and conditions of the contract that will be entered subsequently (within 15 days)and / or in the performance thereof. We agree that the decision of Department, whether any breach of any of the terms and conditions of the contract and / or in the performance thereof has been committed by the SI and the amount of loss ordamage that has been caused or suffered by Department shall be final and binding on us and the amount of the said loss or damage shall be paid by us forthwith on demand and without demur to\_\_\_\_\_.

We\_\_\_\_Bank, further agree that the guarantee herein contained shall

Remain in full force and effect during the period that would be taken for satisfactory performance and fulfilment in all respects of the contract by the SI i.e., till (hereinafter called the said date) and that if any claim accrues or arises against us \_\_\_\_\_ Bank, by virtue of this guarantee before the said date, the same shall been force able against us\_\_\_\_Bank, notwithstanding the fact that the notice of any such claim is given to us Bank, by Department either before the said date or within the enforcement period of six months thereafter. Payment under this letter of guarantee shall be made promptly, within one month of our receipt of notice to that effect from Department.

It is fully understood that this guarantee is effective from the date of the said LoI and that we \_\_\_\_\_Bank, undertaken to revoke this guarantee during its currency without the consent in writing of Department.

We undertake to pay to Department any money so demanded notwithstanding any dispute or disputes raised by the SI inany suit or proceeding pending before any court or Tribunal relating thereto our liability under this present guarantee being absolute and unequivocal. The payment so made by us under this guarantee shall be a valid discharge of our liabilityfor payment there under.

We \_\_\_\_\_ Bank, further agree that\_\_\_\_\_shall have the fullest liberty, without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by theSI from time to time or to postpone for any time or from time to time any of the powers exercisable by against \_\_\_\_\_ the said SI and to forebear or enforce any of the terms and conditions relating to the said contract and we,



Bank, shall not be released from our liability under this guarantee by reason of any such variation or extension being granted to the said SI or for any for bearance by to the said SI or for any for bearance and or omission on the part of or any other matter or thing whatsoever, which under the law relating to sureties, would, but for this provision have the effect of so releasing us from our liability under this guarantee. This guarantee will not be discharged due to the change in the constitution of the Bank or the SI.

Our liability under this Bank Guarantee shall not exceed and is restricted to Rs\_\_\_\_(Rupees\_\_\_\_\_only).

\_\_\_\_\_.Signature of Authorized Signatory (with official seal)

Date :

Place :

Name :

Designation : Address : Telephone &Fax : E-mail address:

\_\_\_\_\_

\_\_\_\_\_

Signature of Witness1

Name \_\_\_\_\_

Signature of Witness2

Name: \_\_\_\_\_

(Bank's common seal)

**10.1.7 Manufacturer's Authorization Form (MAF)/Undertaking from OEM on Authorization of use of their OEM products**

(Company letterhead)

[Date]

To,  
The Director,  
MRSAC, Nagpur

Sub: Authorization of <<company name of System Integrator>> to Provide Services Based on Our Product(s)

Sir,

This is to certify that I / We am / are the Original Equipment Manufacturer in respect of the products listed below. I / We confirm that <name of System Integrator> ("System Integrator") have due authorization from us to provide services, to MRSAC, that are based on our product(s) listed below as per Request for Proposal (RFP) document relating to Selection of System Integrator (SI) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project.

We further certify that the products being quoted (given below) by the SI are of latest model/version and will not be declared as "end-of-sale", "end-of-service" and "end-of-support" within 6 years of publishing of this tender.

We also undertake that support including spares, patches, upgrades/updates, etc. for the quoted products (given below) shall be available for next 5 years from the date of successful installation & acceptance of the project

Sr. No.	Product Name	Model	Make	Country of Origin
1.				
2.				
3.				

Yours faithfully,

Authorized Signatory  
Name  
Designation

OEM's company name

CC: System Integrator's corporate name

## 11 Formats for the Technical Bid Response

### 11.1 Cover Letter to the Technical Proposal

(To be submitted on the Letterhead of the responding firm)

[Date]

To,  
The Director,  
MRSAC, Nagpur

Dear Sir,

Ref: RFP for Selection of System Integrator (S.I) for Selection of System Integrator (SI) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project.

Having examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the professional services as required and outlined in this RFP.

We attach hereto the technical response as required by the RFP, which constitutes our proposal.

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to MRSAC is true, accurate, verifiable, and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the department in its short-listing process.

We fully understand and agree to comply that on verification, if any of the information provided here is found to be misleading the short-listing process, we are liable to be dismissed from the selection process or termination of the contract during the project, if selected to do so.

We agree for unconditional acceptance of all the terms and conditions set out in the RFP document and also agree to abide by this tender response for a period of six months from the date fixed for bid opening.

We hereby declare that in case the contract is awarded to us, we shall submit the performance bank guarantee in the format prescribed in the RFP.

We shall maintain the security and privacy of all data pertaining to the project, including the private data.

We shall submit an agreement with the COTS OEM at the time of signing of contract agreement having validity till the validity of contract agreement signed with MRSAC

We agree that you are not bound to accept any tender response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products / services specified in the tender response.

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.

Dated this \_\_\_\_ Day of 2025

(Signature) (In the capacity of) (Name)

Duly authorized to sign the Tender Response for and on behalf of:

(Name and Address of Company)

Seal/Stamp of SI

Witness Signature:

Witness Name:

Witness Address:

#### CERTIFICATE AS TO AUTHORISED SIGNATORIES

I,....., the Company Secretary of....., certify that  
..... who signed the above Bid is authorized to do so and  
bind the company by authority of its board / governing body.

Date:

Signature:

(Company Seal) (Name)

### **11.1.1 Mandatory Undertakings**

(To be submitted on the Letterhead of the responding firm)

Undertaking on Patent Rights

[Date]

To,  
The Director,  
MRSAC, Nagpur

Sub: Undertaking on Patent Rights

Sir,  
I/We as System Integrator/bidder do hereby undertake that none of the deliverables being provided by us is infringing on any patent or intellectual and industrial property rights as per the applicable laws of relevant jurisdictions having requisite competence.

I/We also confirm that there shall be no infringement of any patent or intellectual and industrial property rights as per the applicable laws of relevant jurisdictions having requisite competence, in respect of the equipment, systems or any part thereof to be supplied by us. We shall indemnify MRSAC, against all cost/claims/legal claims/liabilities arising from third party claim in this regard at any time on account of the infringement or unauthorized use of patent or intellectual and industrial property rights of any such parties, whether such claims arise in respect of manufacture or use. Without prejudice to the aforesaid indemnity, the System Integrator shall be responsible for the completion of the supplies including spares and uninterrupted use of the equipment and/or system or any part thereof to MRSAC, and persons authorized by MRSAC, irrespective of the fact of claims of infringement of any or all the rights mentioned above.

If it is found that it does infringe on patent rights, I/We absolve MRSAC, of any legal action.

Yours faithfully,

(Signature of the Authorized signatory of the Bidder)

Name:

Designation:

Seal:

Date:

Place:

### **11.1.2 Undertaking on Provision for Required Storage Capacity**

(To be submitted on the Letterhead of the responding firm)

[Date]

To,  
The Director,  
MRSAC, Nagpur

Sub: Undertaking on Provision for Required Storage Capacity

Sir,

1. I/We as System Integrator do hereby undertake that the proposed storage at the MRSAC On-Premises setup meets the minimum RFP requirements in terms of a minimum usable capacity of XXTB (with XXTB on FC/XXTB on SAS, SSD, NVMe or equivalent drives with storage array (FC) configured on Raid XX configuration) on the day of commissioning the infrastructure.
2. I/We as System Integrator do hereby undertake that the proposed storage at the MRSAC On-Premises setup as per our sizing will be sufficient to meet the RFP requirements.

Yours faithfully,

(Signature of the Authorized signatory of the Bidder)

Name:

Designation:

Seal:

Date:

Place:

### **11.1.3 Undertaking on Compliance and Sizing of Infrastructure**

(To be submitted on the Letterhead of the responding firm)

[Date]

To,  
The Director,  
MRSAC, Nagpur

Sub: Undertaking on Compliance and Sizing of Infrastructure

Sir,

1. I/We as System Integrator do hereby undertake that we have proposed and sized the hardware and all software (including licenses) based on information provided in the RFP document and in accordance with the Service Level requirements and minimum specifications provided for Software licenses, HCI, Servers, SAN Storage, SAN Switch, Anti-Virus, Backup Software, and all components in RFP and assure MRSAC, that the sizing is for all the functionality envisaged in the RFP document.
2. Any augmentation of the proposed IT infrastructure (software, hardware) in order to meet the minimum tender requirements and/or the requisite Service Level requirements given by MRSAC will be carried out at no additional cost to MRSAC.

Yours faithfully,

(Signature of the Authorized signatory of the Bidder)

Name:

Designation:

Seal:

Date:

Place:

#### **11.1.4 Undertaking on Personnel**

(To be submitted on the Letterhead of the responding firm)

[Date]

To,  
The Director,  
MRSAC, Nagpur

Sub: Undertaking on Personnel

Sir,

1. I/We as System Integrator do hereby undertake that those persons whose profiles were part of the basis forevaluation of the bids and have been identified as “Key Personnel” of the proposed team, including ProjectManager for the project management, Systems Engineer, Cyber Security engineer & Network Engineer, shall be deployed during the Project as per our bid submitted in response to the RFP.
2. We undertake that any of the identified “Key Personnel” shall not be removed or replaced without the prior written consent of MRSAC.
3. Under exceptional circumstances, if the Key Personnel are to be replaced or removed, we shall put forwardthe profiles of personnel being proposed as replacements, which will be either equivalent or better than the ones being replaced. However, whether these profiles are better or equivalent to the ones being replaced willbe decided by MRSAC. MRSAC will have the right to accept or reject these substitute profiles.
4. We also undertake to staff the Project with competent team members in case any of the proposed team members leave the Project either due to voluntary severance or disciplinary actions against them.
5. We undertake that the resources should be full time assigned to the project and will not be working simultaneously on other projects.
6. We acknowledge that MRSAC, has the right to seek the replacement of any member of the Project team being deployed by us, based on the assessment of MRSAC, that the person in question is incompetent to carry out the tasks expected of him/her or found that person does not really possess the skills/experience/qualifications as projected in his/her profile or on the ground of security concerns or breach of ethics.
7. In case we assign or reassign any of the team members, we shall be responsible, at our expense, for transferring all appropriate knowledge from personnel being replaced to their replacements within a reasonable time.

Yours faithfully,

(Signature of the Authorized signatory of the Bidder)

Name:

Designation:

Seal:

Date:

Place:



### **11.1.5 Non – Disclosure Agreement (NDA)**

(To be submitted on the Letterhead of the responding firm)

The MRSAC here in after called the “Purchaser” has issued a public notice inviting various organizations to propose for hiring services of an organization for provision of services under the ‘Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project’ (herein after called the “Project”) of the Purchaser; The SI, having represented to the “Purchaser” that it is interested to bid for the proposed Project, The Purchaser and the SI agree as follows:

- i. In connection with the “Project”, the Purchaser agrees to provide to the SI a Detailed Document on the Project vide the Request for Proposal (RFP). The Request for Proposal contains details and information of the Purchaser operations that are considered confidential.
- ii. The SI to whom this Information (Request for Proposal) is disclosed shall:
  - a. Hold such Information in confidence with the same degree of care with which the SI protects its own confidential and proprietary information.
  - b. Restrict disclosure of the Information solely to its employees, agents, and contractors with a need to know such Information and advise those persons of their obligations hereunder with respect to such Information.
  - c. Use the Information only as needed for the purpose of bidding for the Project.
  - d. Except for the purpose of bidding for the Project, not copy or otherwise duplicate such Information or knowingly allow anyone else to copy or otherwise duplicate such Information.
  - e. Undertake to document the number of copies it makes.
  - f. On completion of the bidding process and in case unsuccessful, promptly return to the Purchaser, all Information in a tangible form or certify to the Purchaser that it has destroyed such Information.
- iii. The SI shall have no obligation to preserve the confidential or proprietary nature of any Information which:
  - a. Was previously known to the SI free of any obligation to keep it confidential at the time of its disclosure as evidenced by the SI’s written records prepared prior to such disclosure; or
  - b. Is or becomes publicly known through no wrongful act of the SI; or
  - c. Is independently developed by an employee, agent, or contractor of the SI not associated with the Project and who did not have any direct or indirect access to the Information.
- iv. The Agreement shall apply to all Information relating to the Project disclosed by the Purchaser to the SI under this Agreement.
- v. The Purchaser will have the right to obtain an immediate injunction enjoining any breach of this Agreement, as well as the right to pursue any and all other rights and remedies available at law or inequity for such a breach.
- vi. Nothing contained in this Agreement shall be construed as granting or conferring rights of license or otherwise,

to the SI, in any of the Information. Notwithstanding the disclosure of any information by the Purchaser to the SI, the Purchaser shall retain title and all intellectual property and proprietary rights in the information. No license under any trademark, patent or copyright, or application for same that are now or thereafter may be obtained by such party is either granted or implied by the conveying of information. The SI shall not alter or obliterate any trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the Purchaser on any copy of the Information and shall reproduce any such mark or notice on all copies of such information.

- vii. This Agreement shall be effective from the date the last signature is affixed to this Agreement and shall continue in perpetuity.
- viii. Upon written demand of the Purchaser, the SI shall:
  - a. Cease using the Information,
  - b. Return the Information and all copies, notes or extracts thereof to the Purchaser forth with after receipt of notice, and
  - c. Upon request of the Purchaser, certify in writing that the SI has complied with the obligations set forth in this paragraph.
- ix. This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes any and all prior oral discussions and / or written correspondence or agreements between the parties. This Agreement may be amended or modified only with the mutual written consent of the parties. Neither this Agreement nor any right granted here under shall be assignable or otherwise transferable.
- x. CONFIDENTIAL INFORMATION IS PROVIDED "ASIS" WITH ALL FAULTS. IN NO EVENT SHALL THE PURCHASER BE LIABLE FOR THE ACCURACY OR COMPLETENESS OF THE CONFIDENTIAL INFORMATION.
- xi. This Agreement shall benefit and be binding upon the Purchaser and the SI and their respective subsidiaries, affiliate, successors, and assigns.
- xii. This Agreement shall be governed by and construed in accordance with the Indian laws. For and on behalf of the SI

(Signature of the Authorized signatory of the Bidder)

Name:

Designation:

Seal:

Date:

Place:

### 11.1.6 Team Profiles

(To be submitted on the Letterhead of the responding firm)

*Table 18 Team Profiles*

<b>Format for the Profiles</b>	
Name of the person	
Current Designation/Job Title	
Current job responsibilities	
Proposed Role in the Project	
Proposed Responsibilities in the Project	
Academic Qualifications: <ul style="list-style-type: none"> <li>• Degree</li> <li>• Academic institution graduated from</li> <li>• Year of graduation</li> <li>• Specialization (if any)</li> <li>• Key achievements and other relevant information (if any)</li> </ul>	
Professional Certifications (if any)	
Total number of years of experience	
Number of years with the current company	
Summary of the Professional/Domain Experience	
Past assignment details (For each assignment provide details regarding name of organizations worked for, designation, responsibilities, tenure) Prior Professional Experience covering: <ul style="list-style-type: none"> <li>• Organizations worked for in the past               <ul style="list-style-type: none"> <li>○ Organization name</li> <li>○ Duration and dates of entry and exit</li> <li>○ Designation</li> <li>○ Location(s)</li> <li>○ Key responsibilities</li> </ul> </li> <li>• Prior project experience               <ul style="list-style-type: none"> <li>○ Project name</li> <li>○ Client</li> <li>○ Key project features in brief</li> <li>○ Location of the project</li> <li>○ Designation</li> <li>○ Role</li> <li>○ Responsibilities and activities</li> </ul> </li> <li>• Duration of the Project Please provide only relevant projects.</li> </ul>	

Each profile must be accompanied by the following undertaking from the staff member:

(Alternatively, a separate undertaking with the same format as below with all the names of the proposed profiles should be provided)

#### Certification

I, the undersigned, certify that to the best of my knowledge and belief, this CV correctly describes my qualifications and my experience. I understand that any willful misstatement described herein may lead to my disqualification or dismissal, if engaged.

Signature:

Date:

[Signature of staff member or authorized representative of the staff] Day/Month/Year

Full name of authorized representative:

## 12 Annexures

### Annexure 1: List of Hardware/Software Required

Sr. No.	Component	Quantity
<b>Hardware Components</b>		
1.	Router	2
2.	Link Load Balancer with DDOS	2
3.	Server Load Balancer with WAF	2
4.	Network Firewall	4
5.	Switch Type - I	2
6.	Switch Type - II	10
7.	Switch Type - III	2
8.	Hyper Converged Infrastructure (HCI)	1
9.	Server Type - I	8
10.	SAN switches	2
11.	NVMe SSD Storage (100 TB)	1
12.	Unified Storage System (1 PB)	1
13.	Backup Storage system with Backup software (1.2PB)	1
14.	RACK with KVM & Console	6
15.	LED Monitor: Size 59 cm with compatible adapter, cables, and wall mount kit with matrix switch	4
<b>Software Components</b>		
1.	HIPS (40 applications)	1 Lot
2.	Endpoint detection and response (EDR)	1 Lot
3.	NMS (upto 400 devices) perpetual license	1
4.	Asset Monitoring Software, Asset Management, Patch Management (upto 400 devices) perpetual license	1
5.	Operating System-Windows server 2022 or latest 64 bit	100
6.	Virtualization Software	16

## Annexure 2: Governance Schedule

### 1. Purpose

The purpose of this Schedule is to:

- i. Establish and maintain the formal and informal processes for managing the relationship between the MRSAC and the System Integrator.
- ii. Define the principles that both Parties wish to follow to ensure the delivery of the Services.
- iii. Ensure the continued alignment of the interests of the Parties.
- iv. Ensure that the relationship is maintained at the correct level within each Party.
- v. Create the flexibility to revise and maintain the relationship during the currency of the project.
- vi. Set out the procedure for escalating disputes/disagreements; and
- vii. Enable contract administration and performance management.

### 2. Governance Structure

The project would require a close supervision and appropriate project control for successfully meeting the objectives and its timely completion.

Indicated below are some of the key functions and roles for different components of the proposed governance structure:

- a. **Steering Committee:** This committee shall be formed by department would provide required level of advocacy for the project and set directions which are acceptable to all stakeholders. The role of this steering committee would be to provide strategic direction to the project.
- b. **PMU:** Project Management Unit would comprise of a team of consultants who would be responsible for monitoring all the project implementation, operations, and maintenance activities, on behalf of MRSAC, and provide status reports, risks, etc. PMU would also be responsible for guiding and managing the project activities between both System Integrator and the MRSAC project team.
- c. **Project Manager:** PM will serve as a single-point contact within the institutional framework for the purpose of project monitoring/reporting purposes and should be deployed by the selected System Integrator. The PM will be responsible for day-to-day coordination between PMU and all implementation teams. PM will be responsible for all the activities within the project scope and will report to Project Management Unit/Team. They will be directly responsible for providing periodic project status, tasks schedule and Action Taken Reports (ATRs).
- d. **Delivery Team:** They will be the actual delivery team deployed by the System Integrator and will work on all areas of the implementation phases including handholding IT infrastructure specialist.
- e. They may also constitute of various other teams as required for successful implementation Transition Management
  - At the end of the contract period or during the contract period, if any other agency is identified or selected for providing services related to System Integrator's scope of work, the System Integrator shall be responsible to deliver services defined in scope and maintain SLA

requirements.

- All risk during transition stage shall be properly documented by System Integrator and mitigation measures are planned in advance so as to ensure smooth transition without any service disruption.
- System Integrator shall provide necessary handholding and transition support, which shall include but not limited to, conducting detailed walk-through of the hardware & software (including licenses, project documentation etc.), addressing the queries/clarifications of the new agency, conducting training sessions etc.
- The transition plan along with period shall be mutually agreed between System Integrator and MRSAC when the situation occurs. System Integrator shall be released from the project once successful transition is done meeting the parameters defined for successful transition.

### **Annexure 3: Draft Contract Agreement**

(To be printed on INR 500/- Stamp Paper)

This AGREEMENT is made at , Maharashtra, on this\_\_day of\_ , 2025,

BETWEEN

MRSAC, Govt. of Maharashtra hereinafter referred to as “MRSAC” (which term or expression, unless excluded by or repugnant to the subject or context, shall mean and include its successors-in office and assigns) of the First Part (which term or expression, unless excluded by or repugnant to the subject or context, shall mean and include its successors-in office and assigns) of the FIRST PART.

AND

M/s \_\_\_\_\_, a company registered under the Companies Act, 1956/2013, having its registered office at, hereinafter referred to as “System Integrator”, (which expression unless repugnant to the context therein, shall include its successors, and permitted assignees), of the SECOND PART.

Each individually a “Party” hereto and collectively the “Parties” And whereas MRSAC, GoM published the RFP to seek services of a reputed firm as a System Integrator for “Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project” (hereinafter referred to as the “Project”) for MRSAC, GoM. And where as M/s \_\_\_\_\_ has submitted its proposal to Design, customize, test, implement, operate & maintain the Project ‘Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project’ as per requirements.

And whereas MRSAC and M/s have decided to enter into this Agreement on the terms and conditions stipulated hereinafter.

NOW, THEREFORE, in consideration of the premises covenants and promises contained herein and other good and valuable considerations, the receipt and adequacy of which is hereby acknowledged, the parties intending to be bound legally, IT IS HEREBY AGREED between the Parties as follows:

#### **1. Definitions**

- a) Bid means the tender process conducted by MRSAC and the technical and commercial proposals submitted by the successful SI, along with the subsequent clarifications and undertakings, if any.
- b) Confidential Information means all information including MRSAC Data (whether in written, oral, electronic or other format) which relates to the technical, financial, business affairs, customers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party in the course of or in connection with this CA (including without limitation such information received during negotiations, location visits and meetings in connection with this CA);
- c) Customers means MRSAC.



- d) Deliverables means all the activities related to the setting up and operations of the infrastructure, documents, Software Applications, Source Codes, as defined in the RFP & subsequent Corrigendum (if any), based on which the technical proposal & commercial proposal was submitted by the System Integrator and as required as per this CA.
- e) Effective Date means the date on which this CA is executed.
- f) CA means this Contract Agreement, together with the recitals and all schedules and the contents, requirements, specifications, and standards of the RFP (as maybe amended, supplemented, or modified in accordance with the provisions hereof) and the Bid. In the event of a conflict between this CA and the schedules, the terms of the CA shall prevail; with overriding effect.
- g) Performance Security means the irrevocable and unconditional Bank Guarantee provided by the System Integrator from a Nationalized Bank/Scheduled Bank other than Co-operative Bank in favor of the DIRECTOR, MRSAC, NAGPUR for an amount equivalent to 10% of the total contract value i.e., Rs..... (Rupees only).
- h) Proprietary Information means processes, methodologies, and technical and business information, including drawings, designs, formulae, flow charts, data and computer programs already owned/licensed by either Party or granted by third parties to a Party hereto prior/subsequent to the execution of this MSA.
- i) Required Consents means the written consents, clearances and licenses, rights and other authorizations as may be required to be obtained by the System Integrator, for all tasks/activities/software/hardware and communication technology for this project; from all the concerned Departments/agencies, etc. as the case maybe.
- j) Service Level(s) means the performance standards, which will apply, to the services delivered through the Software application & hardware implemented by the System Integrator.
- k) Service Level Requirement(s) means the timelines and the quality levels to be adhered to by the System Integrator for delivering various services under the contract.
- l) Services means the content and services delivered and to be delivered to the customers or the Department's offices by the System Integrator and includes but not limited to the services specified in the RFP document or as may be specified and incorporated in the subsequent Agreement/s under Contract Agreement.
- m) Users means the MRSAC staff/officials.

## 2. Interpretation

- a) References to any statute or statutory provision include a reference to that statute or statutory provision as from time to time amended, extended, re-enacted, or consolidated and to all statutory instruments made pursuant to it.

- b) Words denoting the singular shall include the plural and vice-versa and words denoting persons shall include firms and corporations and vice versa.
- c) Unless otherwise expressly stated, the words "herein", "hereof", "hereunder" and similar words refer to this CA as a whole and not to any particular Article, Schedule. The term Articles, refers to Articles of this CA. The words "include" and "including" shall not be construed as terms of limitation. The words "day" and "month" mean "calendar day" and "calendar month" unless otherwise stated. The words "writing" and "written" mean "in documented form", whether electronic or hardcopy, unless otherwise stated.
- d) The headings and use of bold type in this CA are for convenience only and shall not affect the interpretation of any provision of this CA.
- e) The Schedules to this CA form an integral part of this CA and will be in full force and effect as though they were expressly set out in the body of this CA.
- f) Reference at any time to any agreement, deed, instrument, license, or document of any description shall be construed as reference to such agreement, deed, instrument, license, or other document as the same may be amended, varied, supplemented, modified, or suspended at the time of such reference.
- g) Any word or expression used in this CA shall, unless defined or construed in this CA, bear its ordinary English language meaning.
- h) The damages payable by a Party to the other Party as set forth in this CA, whether on per diem basis or otherwise, are mutually agreed genuine pre-estimated loss and liquidated damages likely to be suffered and incurred by the Party entitled to receive the same and are not by way of penalties.
- i) This CA shall operate as a legally binding agreement specifying the master terms, which apply to the Parties under this agreement and to the provision of the services by the System Integrator.
- j) The Department may nominate a technically competent agency / individual(s) for conducting acceptance testing and certification of the various requisite infrastructure to ensure a smooth, trouble free and efficient functioning of the Scheme or carry out these tasks itself.
- k) The agency/individual nominated by the Department can engage professional organizations for conducting specific tests on the software, hardware, networking, security, and all other aspects.
- l) The agency/individual will establish appropriate processes for notifying the System Integrator of any deviations from the norms, standards, or guidelines at the earliest instance after taking cognizance of the same to enable the System Integrator to take corrective action.
- m) Such an involvement of and guidance by the agency/person will not, however, absolve the System Integrator of the fundamental responsibility of designing, customizing, installing, testing, and commissioning the infrastructure for efficient and effective delivery of services as contemplated under

this RFP.

- n) The documents forming this Agreement are to be taken as mutually explanatory of one another. The following order shall govern the priority of documents constituting this Agreement, in the event of a conflict between various documents, the documents shall have priority in the following order:
- i. This Agreement.
  - ii. Scope of Services for the SI
  - iii. Detail Commercial proposal of the SI accepted by MRSAC
  - iv. Clarification & Corrigendum Documents published by MRSAC subsequent to the RFP for this work
  - v. RFP Document of MRSAC for this work
  - vi. LoI issued by the GoM to the successful SI and
  - vii. Successful SI's "Technical Proposal" and "Commercial Proposal" submitted in response to the RFP.

### 3. Term of the Agreement

The term of this CA shall be a period of 5 years and 3 months from the date of execution of this Agreement. This includes the estimated period of 3 months for implementation of the project and 60 months of maintenance & support period.

In the event of implementation period getting extended beyond 3 months, for reasons not attributable to the System Integrator, MRSAC reserves the right to extend the term of the Agreement by corresponding period to allow validity of contract for 60 months from the date of successful go live.

MRSAC, also reserves the right to extend the contract at its sole discretion for duration of 2 years, beyond the initial 5-year period.

### 4. Fees

Total fees to be paid to the System Integrator for the execution of this Contract are into 3 categories as mentioned below:

The fees shall be inclusive of GST, duties, fees, levies, charges as applicable under the relevant Laws of India. Should there be a change in applicable taxes, the actual taxes on the date of billing would prevail.

### 5. Professional Project Management

System Integrator shall execute the project with complete professionalism and full commitment to the scope of work and the prescribed service levels. System Integrator shall attend regular Project Review Meetings called by MRSAC and shall adhere to the directions given during the meeting. Following responsibilities are to be executed by the System Integrator in regular manner to ensure the proper management of the project:

- a) Finalization of the Project plan in consultation with MRSAC and its consultant. Project Plan should consist of work plan, communication matrix, timelines, Quality Plan, Configuration Management Plan, etc.
- b) Plan and deploy the resources in conjunction with the Project Plan and to execute roles and responsibilities against each activity of the project plan
- c) Preparation & regular updation of the Risk Register and the Mitigation Plan. Timely communication of the same to all the identified project stake holders
- d) Submission of Weekly Project Progress Reports
- e) Monthly Compliance report, which will cover compliances to Project Timelines, Project Team, Software/hardware delivered, SLAs, etc.

6. Use & Acquisition of Assets during the term System Integrator shall

- a) Take all reasonable & proper care of the entire hardware & software, network or any other information technology infrastructure components used for the project & other facilities leased/owned by the System Integrator exclusively in terms of the delivery of the services as per this CA (hereinafter the “Assets”) in proportion to their use & control of such Assets which will include all upgrades/enhancements & improvements to meet the needs of the project arising from time to time.
- b) Term “Assets” also refers to all the hardware/Software/furniture/data/documentations /manuals/catalogues/brochures/or any other material procured, created, or utilized by the System Integrator or MRSAC for the Project.
- c) Keep all the tangible Assets in good & serviceable condition (reasonable wear & tear excepted) and/or the intangible Assets suitably upgraded subject to the relevant standards as stated in the RFP to meet the SLAs mentioned in the contract & during the entire term of the Agreement.
- d) Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of Assets & which are provided to the System Integrator will be followed by the System Integrator & any person who will be responsible for the use of the Asset.
- e) Take such steps as may be recommended by the manufacturer of the Assets & notified to the System Integrator or as may be necessary to use the Assets in a safe manner.
- f) To the extent that the Assets are under the control of the System Integrator, keep the Assets suitably housed & conform with any statutory requirements from time to time applicable to them.
- g) Not, knowingly, or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to law.
- h) Use the Assets exclusively for the purpose of providing the Services as defined in the contract.

- i) System Integrator shall not use MRSAC data provide services for the benefit of any third party, as a service bureau or in any other manner

## 7. Security and safety

- a) The System Integrator shall comply with the directions issued from time to time by MRSAC and the standards related to the security and safety in so far as it applies to the provision of the Services.
- b) System Integrator shall also comply with MRSAC, information technology security and standard policies in force from time to time as applicable.
- c) System Integrator shall use reasonable endeavors to report forthwith in writing to all the partners/contractors about the civil and criminal liabilities accruing due to by unauthorized access (including unauthorized persons who are employees of any Party) or interference with MRSAC, data, facilities, or Confidential Information.
- d) The System Integrator shall upon reasonable request by MRSAC or his/her nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.
- e) System Integrator shall promptly report in writing to MRSAC any act or omission which they are aware that could have an adverse effect on the proper conduct of safety and information technology security of the IT infrastructure.

## 8. Service Level Agreement (SLA)

MRSAC expects perfect and professional approach in the project implementation and its operations. System Integrator is expected to satisfy these expectations of the service levels given in Section 9 of this agreement. Any non-adherence to the SLAs would lead to the penalty, to be calculated as provided as part of SLA.

## 9. Indemnity

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

- i. Any misstatement or any breach of any representation or warranty made by the System Integrator  
or
- ii. The failure by the System Integrator to fulfill any covenant or condition contained in this Agreement, including without limitation the breach of any terms and conditions of this Agreement by any employee or agent of the System Integrator. Against all losses or damages arising from claims by third Parties that any Deliverable (or the access, use or other rights thereto), created by System Integrator pursuant to this Agreement, or any equipment, software,

- information, methods of operation or other intellectual property created by System Integrator or sub-contractors pursuant to this Agreement, or the SLAs infringes a copyright, trade mark, trade design enforceable in India, infringes a patent issued in India, or constitutes misappropriation or unlawful disclosure or use of another Party's trade secrets under the laws of India (collectively, "Infringement Claims"); provided, however, that this will not apply to any deliverable (or the access, use or other rights thereto) created by (A) "Implementation of Project by itself or through other persons other than System Integrator or its sub-contractors; (B) Third Parties (i.e., other than System Integrator or sub-contractors) at the direction of MRSAC, or
- iii. Any compensation/claim or proceeding by any third party against MRSAC arising out of any act, deed, or omission by the System Integrator or
  - iv. Claim filed by a workman or employee engaged by the System Integrator for carrying out work related to this Agreement. For the avoidance of doubt, indemnification of Losses pursuant to this section shall be made in an amount or amounts sufficient to restore each of the Indemnified Party to the financial position it would have been in had the losses not occurred.
  - v. Any payment made under this Agreement to an indemnity or claim for breach of any provision of this Agreement shall include applicable taxes.

#### 10. Third Party Claims

- a) Subject to Sub-clause (b) below, the System Integrator (the "Indemnified Party") from and against all losses, claims litigation and damages on account of bodily injury, death or damage to tangible personal property arising in favor of any person, corporation, or other entity (including the Indemnified Party) attributable to the Indemnifying Party's performance or non-performance under this Agreement or the SLAs.
- b) The indemnities set out in Sub-clause (a) above shall be subject to the following conditions:
  - The Indemnified Party, as promptly as practicable, informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise.
  - The Indemnified Party shall, at the cost and expenses of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the defense of such claim including reasonable access to all relevant information, documentation, and personnel. The indemnifying party shall bear cost and expenses and fees of the Attorney on behalf of the Indemnified Party in the litigation, claim.
  - If the Indemnifying Party does not assume full control over the defense of a claim as provided in this Article, the Indemnifying Party may participate in such defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as RFP for Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project for MRSAC, it may deem appropriate, and the cost and expense of the Indemnified Party will be borne and paid by the Indemnifying Party.
  - The Indemnified Party shall not prejudice, pay, or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party.
  - System Integrator hereby indemnify & hold indemnified MRSAC harmless from & against any & all damages, losses, liabilities, expenses including legal fees & cost of litigation in connection with any action, claim, suit, proceedings as if result of claim made by the third party directly or indirectly arising

out of or in connection with this agreement.

- All settlements of claims subject to indemnification under this Article will: (a) be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld & include an unconditional release to the Indemnified Party from the claimant for all liability in respect of such claim; & (b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement.
- The Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings; &
- In the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights & defenses of the Indemnified Party with respect to the claims to which such indemnification relates.
- In the event that the Indemnifying Party is obligated to indemnify the Indemnified Party pursuant to this Article, the Indemnified Party will be entitled to invoke the Performance Bank Guarantee, if such indemnity is not paid, either in full or in part, & on the invocation of the Performance Bank Guarantee, the Indemnifying Party shall be subrogated to all rights & defenses of the Indemnified Party with respect to the claims to which such indemnification relates.

## 11. Publicity

Any publicity by the System Integrator in which the name of MRSAC is to be used should be done with the explicit written permission of the MRSAC.

## 12. Warranties

a. The System Integrator warrants and represents to MRSAC that:

- i. It has full capacity and authority and all necessary approvals to enter into and to perform its obligations under this Agreement.
- ii. This Agreement is executed by a duly authorized representative of the System Integrator.
- iii. It shall discharge its obligations under this Agreement with due skill, care, and diligence so as to comply with the service level agreement.

b. In the case of the SLAs, the System Integrator warrants and represents to MRSAC, that:

- i. The System Integrator has full capacity and authority and all necessary approvals to enter into and to perform its obligations under the SLAs and to provide the Services.
- ii. The SLAs shall be executed by a duly authorized representative of the System Integrator.
- iii. The Services will be provided and rendered by appropriately qualified, trained, and experienced personnel as mentioned in the RFP.
- iv. System Integrator has and will have all necessary licenses, approvals, consents of third Parties free from any encumbrances and all necessary technology, hardware, and software to enable it to provide the Services.

- v. The Services will be supplied in conformance with all laws, enactments, orders, and regulations applicable from time to time.
  - vi. System Integrator will warrant that the goods supplied under the contract are new, of the most recent higher version/models and incorporate all recent improvements in design and materials unless provided otherwise in the contract.
  - vii. The System Integrator shall ensure defect free operation of the entire IT infrastructure and shall replace any such components, equipment, software, and hardware which are found defective and during the entire contract period the System Integrator shall apply all the latest upgrades/patches/releases for the software after appropriate testing. No additional costs shall be paid separately for the warranty other than what are the costs quoted by the System Integrator and as specified in the contract.
  - viii. If the System Integrator uses in the course of the provision of the Services, components, equipment, software, and hardware manufactured by any third party and which are embedded in the Deliverables or are essential for the successful use of the Deliverables, it will pass-through third-party manufacturer's Warranties relating to those components, equipment, software, and hardware to the extent possible.
- c. Notwithstanding what has been stated elsewhere in this Agreement and the Schedules attached herein, in the event the System Integrator is unable to meet the obligations pursuant to the implementation of the Project, Operations and Maintenance Services and any related scope of work as stated in this Agreement and the Schedules attached here in, MRSAC will have the option to invoke the Performance Guarantee after serving a written notice of thirty (30) days on the System Integrator.

### 13. Force Majeure

The System Integrator shall not be liable for forfeiture of its Performance Guarantee, imposition of liquidated damages or termination for default, if and to the extent that its delays in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. For purposes of this Clause, "Force Majeure" means an event beyond the "reasonable" control of the System Integrator, not involving the System Integrator's fault or negligence and not foreseeable. Such events may include Acts of God & acts of Government of India in their sovereign capacity.

For the System Integrator to take benefit of this clause it is a condition precedent that the System Integrator must promptly notify MRSAC, in writing of such conditions and the cause thereof within 5 calendar days of the Force Majeure event arising. MRSAC shall study the submission of the System Integrator and inform whether the situation can be qualified one of Force Majeure. Unless otherwise directed by MRSAC in writing, the System Integrator shall continue to perform its obligations under the resultant Agreement as far as it is reasonably practical and shall seek all reasonable alternative means for performance of services not prevented by the existence of a Force Majeure event.

In the event of delay in performance attributable to the presence of a force majeure event, the time for performance shall be extended by a period(s) equivalent to the duration of such delay. If the duration of delay continues beyond a period of 30 days, MRSAC and the System Integrator shall hold consultations



with each other in an endeavor to find a solution to the problem.

Notwithstanding anything to the contrary mentioned above, the decision of MRSAC shall be final and binding on the System Integrator.

#### 14. Resolution of Disputes

MRSAC and the System Integrator shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the Agreement. If after 30 days from the commencement of such informal negotiations, MRSAC and the System Integrator are unable to resolve amicably such dispute, the matter shall be referred to two Arbitrators: one Arbitrator to be nominated by MRSAC and the other one to be nominated by the System Integrator. In the case of the said Arbitrators not agreeing, then the matter will be referred to an umpire to be appointed by the Arbitrators in writing before proceeding with the reference. The award of the Arbitrators, and in the event of their not agreeing, the award of the Umpire appointed by them shall be final and binding on the parties. Proceedings under this clause shall be subject to applicable law of the Arbitration and Reconciliation Act, 1996. Cost of arbitration shall be borne by each party proportionately. However, expenses incurred by each party in connection with the preparation, presentation shall be borne by the party itself. The provisions of this clause shall survive termination of this Agreement.

#### 15. Risk Purchase Clause

In the event System Integrator fails to execute the project as stipulated in the CA, or as per the directions given by MRSAC from time to time, MRSAC reserves the right to procure similar services from the next eligible System Integrator or from alternate sources at the risk, cost, and responsibility of the System Integrator. Before taking such a decision, MRSAC shall serve a notice period of 1 month to the System Integrator. System Integrator's liability in such case would not be higher than 50% of the contract value.

#### 16. Limitation of Liability towards MRSAC

The System Integrator's liability under the resultant Agreement shall be determined as per the Law in force for the time being. The System Integrator shall be liable to MRSAC for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the System Integrator and its employees, including loss caused to MRSAC on account of defect in goods or deficiency in services on the part of System Integrator or his agents or any person/persons claiming through or under said System Integrator. However, such liability of System Integrator shall not exceed the total value of the Agreement.

#### 17. Conflict of Interest

The System Integrator shall disclose to MRSAC in writing, all actual and potential conflicts of interest that exist, arise, or may arise (either for the System Integrator or its Team) in the course of performing the Services as soon as it becomes aware of such a conflict. System Integrator shall hold MRSAC interest paramount, without any consideration for future work, and strictly avoid conflict of interest with other assignments.

#### 18. Data Ownership

All the data created as the part of the project shall be owned by MRSAC. The System Integrator shall take utmost care in maintaining security, confidentiality, and backup of this data. Access to the data/systems shall be given by the System Integrator only to the personnel working on the projects and their names & contact details shall be shared with MRSAC in advance. MRSAC/its authorized representative(s) shall conduct periodic/surprise security reviews and audits, to ensure the compliance by the System Integrator to data/system security.

## 19. Fraud and Corruption

MRSAC requires that System Integrator must observe the highest standards of ethics during the execution of the contract. In pursuance of this policy, MRSAC defines, for the purpose of this provision, the terms set forth as follows:

- i. "Corrupt practice" means the offering, giving, receiving, or soliciting of anything of value to influence the action of MRSAC in contract executions.
- ii. "Fraudulent practice" means a mis-presentation of facts, in order to influence a procurement process or the execution of a contract, to MRSAC, and includes collusive practice among System Integrators (prior to or after Proposal submission) designed to establish Proposal prices at artificially high or non- competitive levels and to deprive MRSAC of the benefits of free and open competition.
- iii. "Unfair trade practices" means supply of services different from what is ordered on or change in the Scope of Work which is given by MRSAC.
- iv. "Coercive Practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract.

If it is noticed that the System Integrator has indulged into the Corrupt/Fraudulent/Unfair/Coercive practices, it will be a sufficient ground for MRSAC for termination of the contract and initiate blacklisting of the vendor.

## 20. Exit Management

### (i) Exit Management Purpose

This clause sets out the provisions, which will apply during Exit Management period. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Clause.

The exit management period starts, in case of expiry of contract, at least 6 months prior to the date when the contract comes to an end or in case of termination of contract, on the date when the notice of termination is sent to the System Integrator. The exit management period ends on the date agreed upon by MRSAC or 6 months after the beginning of the exit management period, whichever is earlier. The SI must submit a formal letter to MRSAC declaring the initiation date of exit management period.

### (ii) Confidential Information, Security and Data

System Integrator will promptly on the commencement of the exit management period, supply to

MRSAC or its nominated agencies the following:

- a) Information relating to the current services rendered and performance data relating to the performance of the services; Documentation relating to the Project, Project's Intellectual Property Rights; any other data and confidential information related to the Project.
- b) Project data as is reasonably required for purposes of the Project or for transitioning of the services to its Replacing Successful SI in a readily available format.
- c) All other information (including but not limited to documents, records, and agreements) relating to the services reasonably necessary to enable MRSAC and its nominated agencies, or its Replacing Vendor to carry out due diligence in order to transition the provision of the Services to MRSAC or its nominated agencies, or its Replacing Vendor (as the case maybe).

(iii) Rights of Access to Information

At any time during the exit management period, the System Integrator will be obliged to provide an access of information to MRSAC and/or any Replacing Vendor in order to make an inventory of the Assets (including hardware/Software/Active/passive), documentations, manuals, catalogs, archive data, Livedata, policy documents or any other material related to the project.

(iv) Exit Management Plan

Successful SI shall provide MRSAC with a recommended "Exit Management Plan" within 90 days of signing of the contract, which shall deal with at least the following aspects of exit management in relation to the SLA as a whole and in relation to the Project Implementation, the Operation and Management SLA and Scope of work definition.

- i. A detailed program of the transfer process that could be used in conjunction with a Replacement Vendor including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
- ii. Plans for the communication with such of the Successful System Integrator, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on Project's operations as a result of undertaking the transfer.
- iii. Plans for provision of contingent support to the Project and Replacement Vendor for a reasonable period (minimum one month) after transfer.
- iv. Exit Management Plan shall be presented by the System Integrator to and approved by MRSAC or its nominated agencies.
- v. The terms of payment as stated in the Terms of Payment Schedule include the costs of the System Integrator complying with its obligations under this Schedule.
- vi. During the exit management period, the System Integrator shall use its best efforts to deliver the services.
- vii. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

## 21. Termination of contract

MRSAC may, without prejudice to any other remedy under this Contract and applicable law, reserves the right to terminate for breach of contract by providing a written notice of 30 days stating the reason for default to the System Integrator and as it deems fit, terminate the contract either in whole or in part:

- i. If the System Integrator fails to deliver any or all of the project requirements/operationalization/go-live of project within the time frame specified in the contract; or
- ii. If the System Integrator fails to perform any other obligation(s) under the contract.

Prior to providing a notice of termination to the System Integrator, MRSAC shall provide the System Integrator with a written notice of 30 days instructing the System Integrator to cure any breach/default of the Contract, if

MRSAC is of the view that the breach may be rectified. On failure of the System Integrator to rectify such breach within 30 days, MRSAC may terminate the contract by providing a written notice of 30 days to the System Integrator, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to MRSAC. In such event the System Integrator shall be liable for penalty/liquidated damages imposed by MRSAC.

In the event of termination of this contract for any reason whatsoever, MRSAC is entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective continuity of the services which the System Integrator shall be obliged to comply with and take all available steps to minimize the loss resulting from that termination/breach, and further allow and provide all such assistance to MRSAC and/or succeeding vendor, as may be required, to take over the obligations of the System Integrator in relation to the execution/continued execution of the requirements of this contract.

## 22. Miscellaneous

### a. Confidentiality

"Confidential Information" means all information including Project Data (whether in written, oral, electronic or other format) which relates to the technical, financial and operational affairs, business rules, citizen information, design rights, know-how and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party or its subcontractors (whether a Party to the contract or to the SLA) in the course of or in connection with the contract (including without limitation such information received during negotiations, location visits and meetings in connection with the contract or to the SLA) or pursuant to the contract to be signed subsequently.

Except with the prior written permission of MRSAC, the System Integrator and its Personnel shall not disclose such confidential information to any person or entity not expected to know such information by default of being associated with the project, nor shall the System Integrator and its Personnel make public the recommendations formulated in the course of, or as a result of the Project.

The System Integrator recognizes that during the term of this Agreement, sensitive data will be procured & made available to it, its Subcontractors & agents & others working for or under the System Integrator. Disclosure or usage of the data by any such recipient may constitute a breach of law applicable causing harm not only to the Department whose data is used but also to its stakeholders. System Integrator needs to demonstrate utmost care, sensitivity & strict confidentiality. Any breach of this Article will result in MRSAC & its nominees receiving a right to seek injunctive relief & damages, from the System Integrator.

The restrictions of this Article shall not apply to confidential Information that:

- i. is or becomes generally available to the public through no breach of this Article by the Recipient; &
- ii. was in the recipient's possession free of any obligation of confidence prior to the time of receipt of the Recipient hereunder; &
- iii. is developed by the Recipient independently of any of discloser's Confidential Information.
- iv. Is right fully obtained by the Recipient from third Parties authorized at that time to make such disclosure without restriction; &
- v. is identified in writing by the Discloser as no longer proprietary or confidential; or
- vi. is required to be disclosed by law, regulation, or Court Order, provided that the recipient gives prompt written notice to the Discloser of such legal & regulatory requirement to disclose so as to allow the Discloser reasonable opportunity to contest such disclosure.

To the extent that such disclosure is required for the purposes of this Agreement, either Party may disclose Confidential Information to:

- i. its employees, agents & independent contractors & to any of its affiliates & their respective independent contractors or employees; &
- ii. its professional advisors & auditors, who require access for the purposes of this Agreement, whom the relevant Party has informed of its obligations under this Article & in respect of whom the relevant Party has informed of its obligations under this Article has used commercially reasonable efforts to ensure that they are contractually obliged to keep such Confidential Information confidential on terms substantially the same as set forth in this Article. Either Party may also disclose confidential Information or any entity with the other Party's prior written consent.
- iii. The provisions of this Article shall survive the expiration or any earlier termination of this Agreement.

#### b. Standards of Performance

The System Integrator shall provide the services and carry out their obligations under the Contract with due diligence, efficiency, and professionalism/ethics in accordance with generally accepted professional standards and practices. The System Integrator shall always act in respect of any matter relating to this contract. The System Integrator shall abide by all the provisions/Acts/Rules/Regulations, Standing orders, etc. of Information Technology as prevalent in the country. The System Integrator shall also conform to the standards laid down by Government of Maharashtra or Government of India from time to time.

#### c. Subcontracts

All the personnel working on the project and having access to the Servers/data should be on payroll of the

System Integrator. No subcontracting is allowed for the supply, installation, commissioning, and maintenance of any of the hardware and software items listed in section 7.0 of this RFP.

d. Care to be taken while working at MRSAC

System Integrator should follow instructions issued by concerned Competent Authority from time to time for carrying out work at designated places. System Integrator should ensure that there is no damage caused to any private or public property. In case such damage is caused, System Integrator shall immediately bring it to the notice MRSAC in writing and pay necessary charges towards fixing of the damage. System Integrator shall ensure that its employees/representatives don't breach privacy of any employee of MRSAC/Worker or establishment during the course of execution or maintenance of the project.

e. Compliance with Labor regulations

The System Integrator shall pay fair and reasonable wages to the workmen employed, for the contract undertaken and comply with the provisions set forth under the Minimum wages Act and the Contract Labor Act 1970. The salary of the manpower working on this project should be paid using ECS/NEFT/RTGS. A record of the payments made in this regard should be maintained by the System Integrator. Upon request, this record shall be produced to the appropriate authority in State Government and/or Judicial Body. If complaints are received by Government of Maharashtra (or any appropriate authority) appropriate action (Liquidation of Security Deposit, Blacklisting, etc.) may be initiated as deemed necessary against the System Integrator.

f. Independent Contractor

Nothing in this Agreement shall be construed as establishing or implying any partnership or employment relationship between the Parties to this Agreement. Except as expressly stated in this Agreement nothing in this Agreement shall be deemed to constitute any Party as the agent of any other Party or authorizes either Party (i) to incur any expenses on behalf of the other Party, (ii) to enter into any engagement or make any representation or warranty on behalf of the other Party, (iii) to pledge the credit of or otherwise bind or oblige the other Party, or (iv) to commit the other Party in any manner whatsoever in each case without obtaining the other Party's prior written consent.

g. Waiver

A waiver of any provision or breach of this Agreement must be in writing and signed by an authorized official of the Party executing the same. No such waiver shall be construed to affect or imply a subsequent waiver of the same provision or subsequent breach of this Agreement.

h. Notices

Any notice or other document, which may be given by either Party under this Agreement, shall be given in writing in person or by pre-paid recorded delivery post.

In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below

MRSAC, Maharashtra State, Nagpur

<Address> .....

Tel:\_\_\_\_\_

Fax:\_\_\_\_-\_\_\_\_-\_\_\_\_-

System Integrator:

----- RFP for Selection of System Integrator (S.I) for Supply, Installation, Testing, Commissioning of IT Hardware & Software for five years at MRSAC under MahaBHUMI Project.

- -

Tel:\_\_\_\_\_

Fax:\_\_\_\_-\_\_\_\_-\_\_\_\_-

Any notice or other document shall be deemed to have been given to the other Party when delivered (if delivered in person) if delivered between the hours of 9.46 am and 6:15 pm at the address of the other Party set forth above or on the next working day thereafter if delivered outside such hours, and 7 calendar days from the date of posting (if by letter).

i. Personnel/Employees

- i. Personnel/employees assigned by System Integrator to perform the services shall be employees of System Integrator and/or its sub-contractors, & under no circumstances will such personnel be considered as employees of MRSAC. System Integrator shall have the sole responsibility for supervision & control of its personnel & for payment of such personnel 's employee's entire compensation, including salary, legal deductions withholding of income taxes & social security taxes, worker's compensation, employee & disability benefits & the like & shall be responsible for all employer obligations under all laws as applicable from time to time. MRSAC shall not be responsible for the above issues concerning to personnel of the System Integrator.
- ii. System Integrator shall use its best efforts to ensure that sufficient System Integrator personnel are employed to perform the Services, & that, such personnel have appropriate qualifications to perform the Services. MRSAC or its nominated agencies shall have the right to require the removal or replacement of any System Integrator personnel performing work under this Agreement. In the event that MRSAC requests that any System Integrator personnel be replaced, the substitution of such personnel shall be accomplished pursuant to a mutually agreed upon schedule & upon clearance of the personnel based on profile review & upon schedule & upon clearance of the personnel based on profile review & personal interview by MRSAC or its nominated agencies, within not later than 30 working days. System Integrator shall depute a quality team for the project & as per requirements, MRSAC shall have the right to ask System Integrator to change the team.
- iii. Management (Regional Head/VP level officer) of System Integrator needs to be involved in the project monitoring & should attend the review meeting at least once a month.
- iv. The profiles of resources proposed by the System Integrator in the technical proposal, which are considered for technical bid evaluation, shall be construed as 'Key Personnel' & the System Integrator shall not remove such personnel without the prior written consent of MRSAC. For any changes to the proposed resources, System Integrator shall provide equivalent or more experienced resources in consultation with MRSAC.
- v. Except as stated in this clause, nothing in this Agreement will limit the ability of System Integrator freely to assign or reassign its employees; provided that System Integrator shall be responsible, at its expense, for transferring all appropriate knowledge from personnel being replaced to their replacements.

MRSAC shall have the right to review & approve System Integrator's plan for any such knowledge transfer. System Integrator shall maintain the same standards for skills & professionalism among replacement personnel as in personnel being replaced.

- vi. Each Party shall be responsible for the performance of all its obligations under this Agreement & shall be liable for the acts & omissions of its employees & agents in connection therewith.

j. Variations & Further Assurance

- i. No amendment, variation or other change to this Agreement or the SLAs shall be valid unless made in writing & signed by the duly authorized representatives of the Parties to this Agreement.
- ii. Each Party to this Agreement or the SLAs agree to enter into or execute, without limitation, whatever other agreement, document, consent & waiver & to do all other things which shall or may be reasonably required to complete & deliver the obligations set out in the Agreement or the SLAs.
- iii. Severability & Waiver

if any provision of this Agreement or the SLAs, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid, or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the SLAs or the remainder of the provisions in question which shall remain in full force & effect. The relevant Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid, or unenforceable provision a valid & enforceable provision which achieves to the greatest extent possible the economic, legal & commercial objectives of the illegal, invalid, or unenforceable provision or part provision within 7 working days.

- iv. No failure to exercise or enforce & no delay in exercising or enforcing on the part of either Party to this Agreement or the SLAs of any right, remedy or provision of this Agreement or the SLAs shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of any other right, remedy or provision.
- v. Survivability

The termination or expiry of this Agreement or the SLAs for any reason shall not affect or prejudice any terms of this Agreement, or the rights of the Parties under them which are either expressly or by implication intended to come into effect or continue in effect after such expiry or termination.

23. Applicable Law

The contract shall be governed by the laws and procedures prescribed by the Laws prevailing and in force in India, within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/processing. All legal disputes are subject to the jurisdiction of Nagpur court only.

The stamp duty payable for the contract shall be borne by the System Integrator.

IN WITNESS whereof the parties hereto have signed this on the day, month, and year first herein above



written.

Signed, sealed, and delivered

By

\_\_\_\_\_-\_\_\_\_\_-\_\_\_\_\_.

For and on behalf of MRSAC, Government of Maharashtra Signed, sealed, and delivered . . . . .

By\_\_\_\_\_-\_\_\_\_\_-\_\_\_\_\_.

For and on behalf of the “SI”,

- - -

Witnesses :

(1)

(2)

Attachments to the Agreement:

- i. Detail Commercial proposal of the System Integrator accepted by MRSAC
- ii. Corrigendum Document published by MRSAC subsequent to the RFP for this work
- iii. RFP Document of MRSAC for this work
- iv. LoI issued by MRSAC to the successful SI
- v. The successful SI's “Technical Proposal” and “Commercial Proposal” submitted in response to the RFP
- vi. Scope of Services for the System Integrator

## **Annexure 4: Formats for the Commercial Bid Response**

### **Annexure 4A: Cover Letter to Commercial Proposal**

[Date]

To,  
The Director,  
MRSAC, Nagpur

Dear Sir,

I / We, the undersigned, offer to provide the services in accordance with your Request for Proposal vide No.- \_\_\_\_\_ DATED \_\_\_\_\_ and our Technical Proposal. Our attached Commercial Proposal is for the sum of [Insert amount(s) in words and figures]. This amount is inclusive of all taxes.

We hereby confirm that the commercial proposal is unconditional, and we acknowledge that any condition attached to commercial proposal shall result in rejection of our Commercial proposal. Our Commercial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the proposal.

If our proposal is accepted, we will obtain necessary bank guarantee in the format given in the RFP issued by a bank in India, acceptable to MRSAC.

We agree for unconditional acceptance of all the terms and conditions in the bid document and also agree to abide by this bid response for a period of 180 days from the date of submission of bids and it shall be valid proposal till such period with full force and virtue. Until within this period a formal contract is prepared and executed, this bid response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and MRSAC. We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules, and other documents and instruments delivered or to be delivered to MRSAC is true, accurate, and complete. This proposal includes all information necessary to ensure that the statements there in do not in whole or in part mislead MRSAC as to any material fact.

We agree that you are not bound to accept any proposal you receive.

It is hereby confirmed that I/We are entitled to act on behalf of our company/corporation/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this      Day of 2025

(Signature)

(In the capacity of) (Name)

Duly authorized to sign the Tender Response for and on behalf of:

(Name and Address of Company)

Seal / Stamp of SI

Witness Signature:

Witness Name:

Witness Address:

#### CERTIFICATE AS TO AUTHORISED SIGNATORIES

I,,....., the Company Secretary of....., certify that  
..... who signed the above Bid is authorized to do so and  
bind the company by authority of its board / governing body.

Date:

Signature:

(Company Seal) (Name)

**Annexure 4B: Bill of Quantity (BoQ)**

Sr. No.	Item	Ref. Schedule	Total Price (INR)
<b>Capital Cost CAPEX</b>			
(a)	Hardware	A	
(b)	Supporting Software	B	
(c)	Training (Pre-Go-Live)	C	
(i)	Total CAPEX		
<b>Operational Cost OPEX for 5 years</b>			
(d)	Annual Maintenance Cost/warranty	D	
(e)	Human Resource	E	
(ii)	Total OPEX		
<b>Grand Total (i+ii) in figures</b>			
<b>Grand Total (i+ii) in words</b>			

**\*Note:**

- This price (summary) will be used for commercial evaluation
- Details of taxes should be provided by SI/bidder whenever requested by MRSAC

### Schedule A – Hardware

The SI/bidder may add/delete components to the format table below to cover all the line items required to be priced for offering the comprehensive solution as per the requirements given in the RFP. The SI shall provide the same Bill of Material (along with quantity) with the technical proposal without any price quotes.

Sr. No.	Component	Quantity
Hardware Components		
1.	Router	2
2.	Link Load Balancer with DDOS	2
3.	Server Load Balancer with WAF	2
4.	Network Firewall	4
5.	Switch Type - I	2
6.	Switch Type - II	10
7.	Switch Type - III	2
8.	Hyper Converged Infrastructure (HCI)	1
9.	Server Type - I	8
10.	SAN switches	2
11.	NVMe SSD Storage (100 TB)	1
12.	Unified Storage System (1 PB)	1
13.	Backup Storage system with Backup software (1.2PB)	1
14.	RACK with KVM & Console	6
15.	LED Monitor: Size 59 cm with compatible adapter, cables, and wall mount kit with matrix switch	4

### Schedule B – Supporting Software

The System Integrator/bidder may add/delete components to the format table below to cover all the line items required to be priced for offering the comprehensive solution as per the requirements given in the RFP. The SI shall provide the same Bill of Material (along with quantity) with the technical proposal without any price quotes.

Sr. No.	Component	Quantity
Software Components		
1.	HIPS (40 applications)	1 Lot
2.	Endpoint detection and response (EDR)	1 Lot
3.	NMS (upto 400 devices) perpetual license	1
4.	Asset Monitoring Software, Asset Management, Patch Management (upto 400 devices) perpetual license	1
5.	Operating System-Windows server 2022 or latest 64 bit	100
6.	Virtualization Software	16

### Schedule C – Training (Pre-Go-Live)

Sr. No.	Particulars	Unit Rate (INR)	Total Amount (INR)	Taxes & Duties (INR)	Total Price (INR)
			A	B	A+B
1	Training on IT infrastructure (HCI, Cyber Security, Network) Usage, Management & Monitoring				

### Schedule D – Annual Maintenance Cost (Post Warranty Period)

The SI/bidder may add/delete components to the format table below to cover all the line items required to be priced for offering the comprehensive solution as per therequirements given in the RFP.

S. No.	Particulars	Qty	Unit Rate (INR)	Year 1 Amount (INR)	Year 2 Amount (INR)	Total Amount-inclusive of applicable taxes & duties (INR)
<b>Hardware Components</b>						
1.	Router: 4 Ports of 1Gbps of Ethernet Base-T port and 4ports of 10 Gbps SFP+ MM port	2				
2.	Link Load Balancer – 4 Ports of 1 Gbps of Ethernet Base-T port and 4 ports of 10 Gbps SFP+ MM with DDOS – 4x1 Gbps Ethernet Base-T Network Interfaces and should support 8x10 Gbps SFP + MM Network Interfaces	2				
3.	Server Firewall – 4 x1Gb Ethernet ports & 4X10 Gbps ports or SFP MM Fibre ports	4				
4.	Switch Type I – L2 Switch: 16 ports of 10 Gbps and 16x40 Gbps QSFP	2				
5.	Switch Type II – 24 nos. 10 Gbps Ethernet Base-T MM, 4 X 25 Gbps SFP28	10				

6.	Switch Type III (HCI) 24 port (25 Gbps SFP28) MM and uplink 4x40 Gbps QSFP/4x100 Gbps QSFP	2				
7.	HCI solution 4x25 GbE SPF 28, 1x1 GbE	1				
8.	Server Load Balancer with WAF – 4 Ports of 1 Gbps of Ethernet Base-T port and 4 ports of 10 Gbps SFP + MM	2				
9.	Server type 1: 2x10 Gbps Ethernet Base-T and 2x25 Gbps SFP28 Windows Datacenter 2021 or latest	8				
10.	SAN switch 24 x 32Gb Ports. 24 x 15M FC	2				
11.	NVMe SSD 100TB: 4x25 Gb SFP28 MM Ethernet ports per controller. Backend connectivity with NVMe	1				
12.	Unified Storage SAN 1 PB with 4x 25 Gbps SFP28 MM + 4x 32 Gbps FC ports available per controller.	1				
13.	Backup storage, system and software 4 x 25 Gbps	1				
14.	Smart RACK (KVM + Console)	6				
15.	LED Monitor: Size 59 cm with compatible adapter, cables, and wall mount kit	4				

**Note:** Additional line item, if required by the SI to meet the scope

#### Software Components

1.	HIPS (40 applications)	1 Lot				
2.	Endpoint detection and response (EDR)	1 Lot				

3.	NMS (upto 400 devices) perpetual license	1 Lot				
4.	Asset Monitoring Software, Asset Management, Patch Management (upto 400 devices) perpetual license	1 Lot				
5.	Operating System – Windows server 2022 or latest 64 bit	100				
6.	Virtualization Software	16				

#### Schedule E – Human Resource

Sr. No	Particulars	Qty	Year 1 Amount (INR)	Year 2 Amount (INR)	Year 3 Amount (INR)	Year 4 Amount (INR)	Year 5 Amount (INR)	Total Amount-inclusive of applicable taxes & duties (INR)
1	Project Manager	1						
2	Systems Engineer	1						
3	Network Engineer	1						
4	Cyber Security Engineer	1						

#### Schedule F – Additional hyperconverged nodes

Sr. No.	Particulars	Quantity	Unit Rate (INR)	Total Amount (INR)	Taxes & Duties (INR)	Total Price (INR)
				A	B	A+B
1	Additional Hyperconverged node	1				

#### Schedule G – Annual Maintenance cost for additional hyperconverged nodes (Post Warranty Period)

Sr. No.	Particulars	Quantity	Unit Rate (INR)	Year 1 Amount (INR)	Year 2 Amount (INR)	Total Amount-inclusive of applicable taxes & duties (INR)
1.	Additional Hyperconverged Node	1				

**Note:** Schedule F & G are only for price discovery purposes. In case MRSAC requires additional hyperconverged nodes for any of the clusters, the same shall be provided by SI at the above rates.





Item Rate BoQ

Tender Inviting Authority: Director, Maharashtra Remote Sensing Application Center (MRSAC)

Name of Work: Selection of System Integrator (S.I) for Supply, Installation, Commissioning, Warranty & Maintenance (for five years) of IT Hardware & Software at MRSAC under MahaBHUMI Project

Contract No: RFP Number: MRSAC/SI/01/2025

Name of the Bidder/ Bidding Firm / Company :							
<p><b>PRICE SCHEDULE</b></p> <p>(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)</p>							
NUMBER #	TEXT #	NUMBER #	TEXT #	NUMBER #	NUMBER #	NUMBER #	TEXT #
Sl. No.	Item Description	Quantity	Units	BASIC RATE in <b>Figures</b> To be entered by the <b>Bidder</b> Rs. P	TOTAL AMOUNT Without Taxes	TOTAL AMOUNT With Taxes	TOTAL AMOUNT In Words
1	2	4	5	13	53	54	55
1	Schedule A – Hardware						
1.01	Router	2	Nos		0.00	0.00	INR Zero Only
1.02	Link Load Balancer with DDOS	2	Nos		0.00	0.00	INR Zero Only
1.03	Server Load Balancer with WAF	2	Nos		0.00	0.00	INR Zero Only
1.04	Network Firewall	4	Nos		0.00	0.00	INR Zero Only
1.05	Switch Type - I	2	Nos		0.00	0.00	INR Zero Only
1.06	Switch Type - II	10	Nos		0.00	0.00	INR Zero Only
1.07	Switch Type - III	2	Nos		0.00	0.00	INR Zero Only
1.08	Hyper Converged Infrastructure (HCI)	1	Nos		0.00	0.00	INR Zero Only
1.09	Server Type - I	8	Nos		0.00	0.00	INR Zero Only
1.10	SAN switches	2	Nos		0.00	0.00	INR Zero Only
1.11	NVMe SSD Storage (100 TB)	1	Nos		0.00	0.00	INR Zero Only
1.12	Unified Storage System (1 PB)	1	Nos		0.00	0.00	INR Zero Only
1.13	Backup Storage system with Backup software (1.2PB)	1	Nos		0.00	0.00	INR Zero Only
1.14	RACK with KVM & Console	6	Nos		0.00	0.00	INR Zero Only
1.15	LED Monitor: Size 59 cm with compatible adapter, cables, and wall mount kit with matrix switch	4	Nos		0.00	0.00	INR Zero Only
2	Schedule B – Supporting Software						
2.01	HIPS (40 applications)	1	Lot		0.00	0.00	INR Zero Only
2.02	Endpoint detection and response (EDR)	1	Lot		0.00	0.00	INR Zero Only
2.03	NMS (upto 400 devices) perpetual license	1	Lot		0.00	0.00	INR Zero Only

2.04	Asset Monitoring Software, Asset Management, Patch Management (upto 400 devices) perpetual license	1	Lot		0.00	0.00	INR Zero Only
2.05	Operating System-Windows server 2022 or latest 64 bit	100	Nos		0.00	0.00	INR Zero Only
2.06	Virtualization Software	16	Nos		0.00	0.00	INR Zero Only
3	Schedule C – Training (Pre-Go-Live)						
3.01	Training on IT infrastructure (HCI, Cyber Security, Network) Usage, Management & Monitoring	2	Nos		0.00	0.00	INR Zero Only
4	Schedule D – Annual Maintenance Cost (Post Warranty Period)						
4.01	Annual maintenance cost post warranty for 2 years	1	Lumpsum		0.00	0.00	INR Zero Only
5	Schedule E – Human Resource						
5.01	Technical human resources for Five Years	1	Lumsum		0.00	0.00	INR Zero Only
6	Schedule F – Additional hyperconverged nodes						
6.01	Additional hyperconverged nodes	1	Nos		0.00	0.00	INR Zero Only
Total in Figures					0.000	0.000	INR Zero Only
Quoted Rate in Words		INR Zero Only					