RAILTEL CORPORATION OF INDIA LIMITED

(A Govt. of India Undertaking, Ministry of Railways)

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

for

"Selection of Managed Service Provider (MSP) for procurement of Cloud services to MRSAC under MahaBhumi project of Govt. of Maharashtra for DC and DR for 5 years."

EOI No: RailTel/WR/B-N/MRSAC (MH)/EOI/2024-25/11 dated 13th Aug. 2024

**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 (MH)/EOI/2024-25/11 dated 13th Aug. 2024

RailTel Corporation of India Ltd., (here after referred to as "RailTel") invites EOIs from RailTel's Empaneled Partners or OEMs or OEM's authorized partner/distributor for the selection of suitable partner for participation for **"Selection of Managed Service Provider (MSP) for procurement of Cloud services to MRSAC under MahaBhumi project of Govt. of Maharashtra for DC and DR for 5 years"**

The details are as under:

1	Last date for submission of EoI response by bidders	16th August 2024 at 16:00 Hours
2	Opening of Bid response packet of EOIs	16th August 2024 at 16:30 Hours
3	Number of copies to be submitted for scope of work	One
4	EMD Amount	Rs. 25,00,000/- (Rupees Twenty Five Lakhs Only)
5	Tender Fees & Processing Fees	Rs. 25000/-

The EMD should be in the favor of RailTel Corporation of India Limited payable at Mumbai through online bank transfer. Partner needs to share the online payment transfer details like UTR No. date and Bank along with the proposal.

RailTel Bank Details: Union Bank of India, Account No.317801010036605, IFSC Code - UBIN0531782, Branch name – Mahalaxmi Branch

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

Level:1 Contact: Sh. Anand Kumar
Position: Jt. General Manager/Marketing
Email: anandnkn@railtelindia.com
Contact: +91-9004444107

Level:2 Contact: Sh. Pavan Kumar Bhargava
Position: ED/TM/Bhopal
Email: pavan@railtelindia.com

Note:

1. Empaneled partners/OEMs/authorized partner or distributor of OEMs are required to submit soft copy (password protected PDF) of bid response packet (separate for Technical bid and Financial Bid) through an e-mail at **bpltooffice@railtelindia.com** duly signed by Authorized Signatories 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 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 of OEM of RailTel for fulfilling the end customer requirements.** Selected partner's authorized signatory has to give an undertaking 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.
6. **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

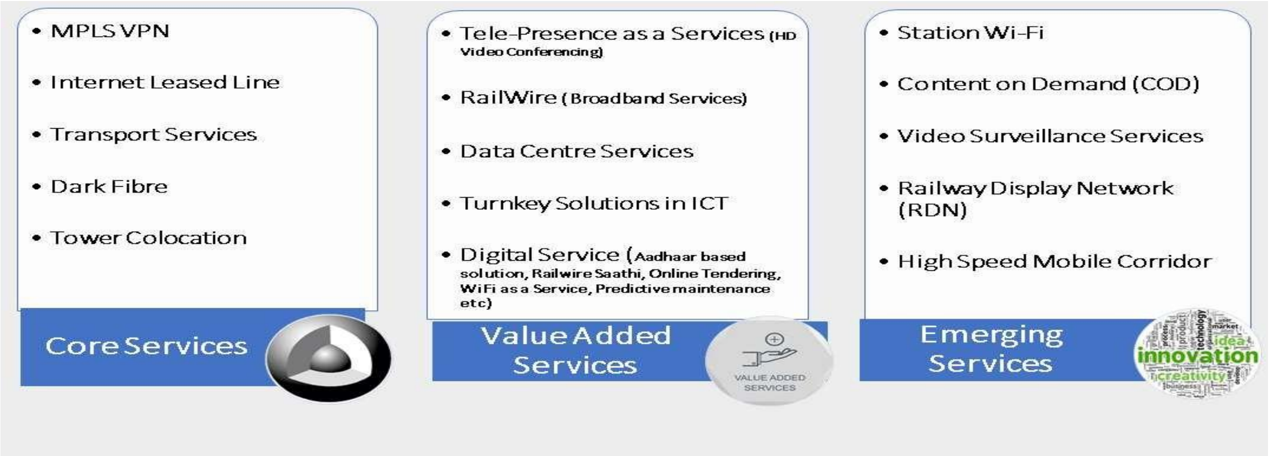
RailTel Corporation of India Limited (RailTel), an ISO-9001:2000 organization is a Class- A Mini-Ratna Government of India undertaking under the Ministry of Railways. The Corporation was formed in Sept 2000 with the objectives to create nationwide Broadband Telecom and Multimedia Network in all parts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

RailTel has approximately 60000 kms of OFC along the protected Railway tracks. The transport network is built on high capacity DWDM and an IP/ MPLS network over it to support mission critical communication requirements of Indian Railways and other customers. RailTel has Tier-III Data Center in Gurgaon and Secunderabad hosting / collocating critical applications. RailTel is also providing Telepresence as a Service (TPaaS), where a High- Definition Video Conference facility bundled with required BW is provided as a Service.

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

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

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:



- MPLS VPN
- Internet Leased Line
- Transport Services
- Dark Fibre
- Tower Colocation

Core Services

- Tele-Presence as a Services (HD Video Conferencing)
- RailWire (Broadband Services)
- Data Centre Services
- Turnkey Solutions in ICT
- Digital Service (Aadhaar based solution, Railwire Saathi, Online Tendering, WiFi as a Service, Predictive maintenance etc)

Value Added Services

- Station Wi-Fi
- Content on Demand (COD)
- Video Surveillance Services
- Railway Display Network (RDN)
- High Speed Mobile Corridor

Emerging Services

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 centres in Gurgaon & Secunderabad. Presently RailTel is hosting critical applications of Indian Railways, Central & State government/ PSUs applications. RailTel will facilitate Government's applications / Hosting services including smooth transition to secured state owned RailTel's Data Centers and Disaster Recovery Centres. RailTel also offers SOC as a Service 'SOCaaS'. In addition, RailTel offers VPN client services so that employees can seamlessly access government's intranet, applications securely from anywhere without compromising security.

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

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

e) **Retail Services – RailWire**

RailWire: Triple Play Broadband Services for the Masses. RailTel has unique model of delivering broadband services, wherein local entrepreneurs are engaged in delivering & maintaining broadband services and upto 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 Managed Service Provider (MSP) for procurement of Cloud services to MRSAC under MahaBhumi project of Govt. of Maharashtra for DC and DR for 5 years”

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 Managed Service Provider (MSP) for procurement of Cloud services to MRSAC under MahaBhumi project of Govt. of Maharashtra for DC and DR for 5 years” 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.

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 90 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 favour 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 can be received in the form of bank Guarantee/Online Bank Transfer/ Fixed Deposit. Bank guarantee has to be confirmed with the Structural Financial Messaging System (SFMS) confirmation from the issuing Bank in favor of RailTel. In case of Fixed Deposit, lien in favor of RailTel is to be ensured. However, EMD amount equal or less than Rs. 5 Lakhs shall be sought only in 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 asper 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 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

Pre-qualification Criteria for Managed Service Provider (MSP):

S. No	Pre-Qualification Criteria	MSP	Documents required substantiating pre- qualifying criteria
1.	The MSP 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. OR Limited Liability Partnership firm registered under Limited Liability Partnership Act, 2008.	Mandatory	Copy of Certificate of Incorporation / Registration Certificate
2.	The MSP should be single partner / firm registered in India. No consortium of firms is allowed.	Mandatory	Copy of Certificate of Incorporation / Registration Certificate
3.	The MSP should be in existence for minimum of 10 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.	Average annual turnover of the last three audited financial years (FY 2020-21, FY 2021-22, FY 2022-23) from IT / ITES / Cloud services	Minimum INR 45 Crores	Audited Balance sheets and Profit & Loss account statements of the MSP for each of the last three audited financial years FY 2020- 21, and FY 2021-22, FY 2022- 23, 1. Certificate duly signed by Statutory Auditor of the MSP or Certified Chartered Accountant for average annual turnover from IT / ITES / Cloud services.
5.	The MSP must have a positive net worth in each of the last 3 financial years	Mandatory	Certificate duly signed by Statutory Auditor of the MSP or Certified Chartered Accountant specifying the net worth of the MSP.
6.	The MSP should possess the following valid certification as on bid submission date: ISO27001, ISO 20000, ISO 27000	Mandatory	Copy of valid certificate of ISO27001, ISO 20000, ISO 27000 as on bid submission date
7.	The MSP, in last 5 years (as on bid submission date) should have undertaken at least One (1) similar Project of Cloud* (establishment of DC/DR with project value of at least Rs. 10 Cr • OR	Mandatory	On Going Project + Invoice Copy or Work order (WO) / Contract document(s) and Completion certificate(s) or Go Live certificate from client or Project Citation in the attached format.

	1) Two similar projects of minimum value of 4.0 Crore each having scope of Application and Data Migration Services to Cloud (At least one project should be of Migration from On prem Physical Infrastructure to Cloud, setting up & hosting of IT infrastructure & systems at Cloud) and providing managed services		All above supporting documents must mandatorily mention the value of project and duration of the contract.
8.	The MSP 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.
9.	The MSP must have valid Goods Tax registration in India & PAN card	Mandatory	Proof of valid Goods Tax Registration in India & Copy of PAN Card
10.	A Board Resolution or Power of Attorney, in the name of the person executing the bid, authorizing the signatory to sign on behalf of the Bidding entity. The person issuing the Power of Attorney shall possess Board Resolution in his favour for granting such rights. In case of generic Board Resolution or Power of Attorney, the same shall be certified by Company Secretary.	Mandatory	As per the format given in Annexure I, Point no. 15.1.3 of this document

Pre-qualification Criteria for Cloud Service Provider (CSP):

S. No	Pre-Qualification Criteria	Documents required substantiating pre- qualifying criteria
1.	The CSP should be registered under Companies Act, 1956 or as amended or an LLP firm / Partnership firm under Partnership Act 1932. The CSP should have an average annual turnover of INR 200 Crores for last three financial years (2020-21, 2021-22, 2022-23) and positive net worth as on 31st March 2023 or as on financial audit date of last financial year with at least 5 years of Operations in India as on bid submission date.	• Copy of Certification of Incorporation / Registration Certificate • Audited Balance sheet and Profit & Loss; for the last three financial years (2020-21, 2021-22, 2022-23) If Audited Balance Sheets and Profit & Loss account statements are not available for FY 2022 –23, then the SI may provide the Certificate duly signed by Statutory Auditor of the SI or Certified Chartered Accountant for average annual turnover • Certificate from the Statutory Auditor / Company Secretary on turnover details for the last three financial years (FY 2020-21, 2021-22, 2022-23) • Certificate from the Statutory Auditor / Company Secretary on positive net-worth for the last three financial years (2020-21, 2021-22, 2022-23)
2.	The CSP should have experience in India of executing minimum 3 (completed / ongoing) projects of DC / DR hosting on Cloud with minimum value of INR 100 Crores for any State or Central Government Institution, with at least one of the implementations involving Hyper scale computing, during the last 5 years as on bid submission date.	• Work Order + Self Certificate of Completion / Ongoing (Certified by the Statutory Auditor / Company Secretary). AND • Contract clearly highlighting the Scope of Work, Bill of Material and value of the Contract / order OR Self-certificate from the CSP mentioning the Scope of Work, Bill of Material and value of the Contract /

		order, signed by Statutory Auditor / Company Secretary of the MSP for this bid
3.	The CSP must be operating at least two (2) Cloud Solution site / disaster recovery site in India in different seismic zones at time of submission of the bid.	Self-certificate from the CSP mentioning the location details signed by authorized signatory of the CSP for this bid
4.	The CSP shall be MeitY's empaneled & STQC audited as per Ministry of Electronics and Information Technology (MeitY) as on bid submission date.	Valid Letter of Empanelment / Certificate of Empanelment from MeitY) including details on STQC audit status
5.	CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and / or privacy Trust Services principles such as SOC 1, SOC 2, SOC 3.	Copies of valid certificates (SOC1, SOC2 and SOC3) as on bid submission date
6.	CSP should possess following mandatorily certifications: ISO 27001:2013 certification ISO / IEC 27017:2015-Code of practice for information security controls based on ISO / IEC 27002 for cloud services and Information technology. ISO 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds ISO 20000-1:2011 certification for Service Management System	Copies of certificates valid as on bid submission date
7.	The CSP or proposed DC-DR facility should not have been blacklisted / debarred by any Central / State Government as on bid submission date (during last five (5) years).	A self-certified letter by the authorized signatory of the MSP that the MSP has not been blacklisted by any Central / State Government (Central / State Government and Public Sector) or under a declaration of ineligibility for corrupt or fraudulent practices as of <bid submission date> must be submitted on original letter head of the MSP with signature and stamp
8.	The proposed Data Centre should be running Government community Cloud (GCC) or Virtual Private Cloud (VPC)	Valid copies of proof attested by authorized signatory
9.	CSP cloud platform must have ability to enable the below listed technology and OEM components on cloud Databases, Repositories and Data Stores: • ArcGIS engine from ESRI • Apollo Server • MySQL Server 8 with GIS / image serving capabilities or above. • PostgreSQL GIS / image serving capabilities)	Certificate and letter from authorized signatory on the letter head of CSP mentioning the compliance

S No.	Particulars	Criteria for Tender Package
		(Mandatory Compliance & Document Submission)
B)	**Annexures**	
ix)	**Annexure 1**	**Covering Letter:** Self-certification duly signed by authorized signatory on company letter head.
x)	**Annexure 2**	The Bidder should agree to abide by all the technical, commercial & financial conditions of the end customer RFP for which EOI is submitted.
		Self-certification duly signed by authorized signatory on company letter head.
xi)	**Annexure 3**	An undertaking signed by the Authorized Signatory of the company to be provided on letter head. The Bidder should not have been blacklisted/ debarred by any Governmental /Non-Governmental Organization in India as on bid submission date.
xii)	**Annexure-4**	Format for Affidavit to be uploaded by BA along with the tender documents.
xiii)	**Annexure-5**	Non-disclosure agreement with RailTel.
xiv)	**Annexure-6**	BOQ of the RFP document. Price Bid Format to be submitted in separate password protected pdf.
xv)	**Power of Attorney**	Power of Attorney and Board Resolution in favor of one of its employees who will sign the Bid Documents.
xvi)	**Additional Documents to be Submitted**	Technical Proposal with overview of the project with strength of the Partner.

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: Format for COVERING LETTER

COVERING LETTER (To be 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

Annexure 2: Format for Self-Certificate & Undertaking

Self-Certificate (To be on company letter head)

EoI Reference No: Date:

To,

RailTel Corporation of India Ltd.
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

<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. 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.

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

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (this "***Agreement***") is made and entered into on this ___________day of ____ , 2024 (the "***Effective Date***") at____. By and between

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

And

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

RailTel and _________shall be individually referred to as "Party" and jointly as "Parties"

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

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

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

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

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.

RailTel Corporation of India limited:

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 Price bid as per the format of the MRSAC Tender

MAHARASHTRA REMOTE SENSING APPLICATION CENTRE
(Autonomous Body of Planning Department, Govt. of Maharashtra)
VNIT Campus, S.A. Road, Nagpur – 440010
Email: admn-mrsac@mrsac.gov.in

CORRIGENDUM NO. 3

DATE: 08-08-2024

Corrigendum No. 3: Pre-bid Response

Corrigendum Reference: RFP Reference Number MRSAC/CLOUD/04/2024-25 dated 18-07-2024 for, **"Request for Proposal for Selection of Managed Service Provider MSP for procurement of Cloud services to MRSAC under MahaBHUMI Project of Govt. of Maharashtra for DC and DR for 5 years"**.

The bidders / applicants are required to kindly consider the following corrigendum pertaining to the aforementioned RFP:

The revised Request for Proposal (RFP) document is attached as **Annexure A**.

All the bidders / applicants are requested and expected to thoroughly read the entire revised RFP document, in order, to understand the entire project's details, scope of work etc. and shall accordingly submit the commercials

Sd/-
Director
MRSAC, Nagpur

ANNEXURE A

REVISED REQUEST FOR PROPOSAL

For Selection of Managed Service Provider (MSP) for providing Cloud services to MAHARASHTRA REMOTE SENSING APPLICATION CENTRE (MRSAC) Under MahaBHUMI Project of Govt. of Maharashtra for DC and DR for 5 years.

RFP Number: MRSAC/CLOUD/04/2024-25

Issued on: 18-07-2024

This page has been intentionally kept blank

Table of Contents

1 Glossary 8

2 Definitions 11

3 Invitation for Proposal 12

4 Fact Sheet.. 15

5 Introduction 17

5.1 About MRSAC 17

5.2 Project Background 17

5.3 Broad Objectives of MahaBHUMI Project.. 17

5.4 MRSAC Requirements 18

5.5 Cloud hosting general requirements 18

5.6 Responsibilities of MSP and CSP 19

5.6.1 Responsibilities of MSP..19

5.6.2 Responsibilities of CSP..20

6 Pre-Qualification.. 21

6.1 Pre-qualification Criteria for Managed Service Provider (MSP): 21

6.2 Pre-qualification Criteria for Cloud Service Provider (CSP): 23

7 Instructions to MSP: 26

7.1 Purpose of Bid Document 26

7.2 Cost of Bid Document.. 26

7.3 Completeness of Bid Document 26

7.4 Proposal Preparation Cost 26

7.5 Bid Cover Letters 26

7.6 Power of Attorney 27

7.7 Pre-Bid Meeting 27

7.8 Amendments to Bid Document 27

7.9 Rights to Terminate the Process.. 27

7.10 Language of Bids 28

7.11 Bid Submission Format.. 28

7.12 Online Bid Submission 28

7.13 Procedure for Submission of Bids 29

7.14 Two Envelope Bid System 30

7.15 Supporting Documents for Bid 30

7.16 Earnest Money Deposit (EMD) and Refund 31

7.17 Evaluation Process 31
7.18 Opening of Bid 31
7.19 Evaluation of Technical Bids 32
7.20 Notifications of Award and Signing of Contract 32
7.21 Failure to agree with the Terms & Conditions of the Bid Document / Contract: 32
7.22 Terms and Conditions of the Tender 32
8 Scope of Work 33
8.1 Detailed scope of work 37
8.1.1 One-time integration Services for Provisioning and Validation of Secure Infrastructure 37
8.1.2 Ongoing infrastructure Managed Services (For the period of Contract) 37
8.1.3 Express Connectivity between Cloud Service Zone and MRSAC Nagpur 39
8.2 Operational Acceptance and Maintenance & Support of Cloud 40
8.3 Resource Management and Service Provisioning: 42
8.4 User Administration and Management: 43
9 Technical Requirements: 44
9.1 Requirement for Cloud: 44
9.2 General Requirement 46
9.3 Compute Requirement: 47
9.4 Storage Requirement 48
9.5 Network Requirement 51
9.6 Security Requirement: 53
9.7 Monitoring Requirements 58
9.8 Usage Reporting and Billing Management 60
10 Disaster Recovery Services 62
10.1 Overview 62
10.2 RPO & RTO Requirements: 62
10.3 Replication Requirements: 63
10.4 Support Third Party Audit and other requirements 65
10.5 Exit Management / Transition-Out Services: 65
10.6 Business Continuity Planning: 65
10.7 Other Requirements: 66
10.8 Project Planning and Management 69
10.9 Schedule of Events: 69
10.10 Technical Terms and Conditions 70
11 Work Completion Timelines & Payment Terms 72

12 Service Level Agreement (SLA) and Penalty Clause 74

13 Technical Qualification 84

13.1 Technical Qualification process 84

13.2 Technical Evaluation Criteria 85

13.3 MSP's Experience 85

13.4 CVs of Resources 85

13.5 Capabilities in service provisioning across CSPs 86

13.6 Technical Presentation 86

14 Draft Contract Agreement 87

14.1 Definitions, Interpretations and Other Terms 87

14.2 Interpretations 87

14.3 Term of the Contract Agreement 89

14.4 Professional Project Management:........ 89

14.5 Use & Acquisition of Assets during the term 89

14.6 Security and Safety 90

14.7 Performance Bank Guarantee 90

14.8 Indemnity 90

14.9 Third Party Claims 91

14.10 Warranties 93

14.11 Force Majeure 93

14.12 Resolution of Disputes 94

14.13 Limitation of Liability towards MRSAC 94

14.14 Conflict of Interest 94

14.15 Data Ownership 95

14.16 Fraud and Corruption 95

14.17 Exit Management 96

14.18 Termination of Contract 99

14.19 Confidentiality 99

14.20 Miscellaneous 100

14.21 Applicable Law 103

15 Annexure I:........ 104

15.1 Instructions for Pre-Qualification Bid........ 104

15.1.1 Pre-Qualification Cover Letter 104

15.1.2 Template for Pre-Bid Queries 104

15.2 Instructions for Technical Bid Document Format 106

15.2.1 Technical Bid Cover Letter (MSP Company letter head) 106

15.2.2 Checklist for the documents to be submitted 107

15.2.3 Format for citations for MSPs Experience 108

15.2.4 Format for citations for CSPs Experience 108

16 Annexure II: 109

16.1 Bill of Material 109

17 Annexure III 113

17.1 Commercial Bid Declaration.................. 113

17.2 Commercial Proposal: 115

17.2.1 Best Price Offer Letter Format 115

17.3 Commercial Bid Format & Instructions.................. 116

17.4 Commercial Bid Format.................. 117

This page has been intentionally kept blank

1 Glossary

Abbreviation	Description
AMC	Annual Maintenance Contract
API	Application Programming Interface
CCN	Change Control Note
CI-CD	Continuous Integration-Continuous Development
CDN	Content Delivery Network
CNS	Change Note on Scope of Work
CPU	Central Processing Unit
CSP	Cloud Service Provider
CSC	Common Service Centre
DC	Data Centre
DCO	Data Centre Operator
DIT	Department of Information Technology
DoS	Denial of Service
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DMZ	Demilitarized Zone
DRaaS	Disaster Recovery-as-a-Service
DSC	Digital Signature Certificate
DR	Disaster Recovery
EMD	Earnest Money Deposit
FAQ	Frequently Asked Question
GST	Goods & Services Tax
HDD	Hard Disk Drive
HIPS	Host Intrusion Prevention System
HIDS	Host Intrusion Detection System
IAM	Identity Access Management
IDS	Intrusion Detection Sensor
INR	Indian Rupees
IOPS	Input / Output Operations Per Second
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISP	Internet Service Provider
ISO	International Organization for Standardization
LLP	Limited Liability Partnership
LAN	Local Area Network
MeitY	Ministry of Electronics and Information Technology
MGDDS	Maharashtra Geo-spatial Digital Database System
MRSAC	Maharashtra Remote Sensing Application Centre
MSP	Managed Service Provider
MPLS	Multiprotocol Label Switching
NDA	Non-Disclosure Agreement

Abbreviation	Description
NIDS	Network Intrusion Detection System
NSP	Network Service Provider
OEM	Original Equipment Manufacturer
PBG	Performance Bank Guarantee
PoC	Proof of Concept
PCI-DSS	Payment Card Industry Data Security Standard
RAM	Random Access Memory
RDBMS	Relational Database Management System
RFP	Request for Proposal
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SDC	State Data Centre
SDD	System Design Documents
SIEM	Security Information and Event Management
SITC	Supply Installation Testing & Commission
SLA	Service Level Agreement
STQC	Standardization Testing and Quality Certification
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
TRAI	Telecom Regulatory Authority of India
UAT	User Acceptance Testing
vCPU	Virtual Central Processing Unit
VLBS	Virtual Load Balancer Services
VM	Virtual Machine
VTL	Virtual Tape library
WAN	Wide Area Network

This page has been intentionally kept blank

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 Governing Body of MRSAC.

ii. "Financial Year" means the year beginning on the 1st of April and ending on the 31st of March of the following year.

iii. "Successful MSP" is the MSP chosen by the project owner to receive award of the contract for performing the said scope of work.

iv. "Managed Service Provider" is an organization that specializes in bringing together component into a whole and ensuring that those subsystems function together.

v. "Net worth" is measured as paid-up capital plus free reserves.

vi. "Department" means Maharashtra Remote Sensing Application Centre

vii. "IT Infrastructure" means hardware & software including networking components (active & passive) provided by the MSP.

viii. "MSP" or "Respondent" is the entity which submits bid as per this RFP.

3 Invitation for Proposal

Maharashtra Remote Sensing Application Centre- MRSAC (Autonomous Body of Planning Department, Govt. Of Maharashtra), VNIT Campus, S.A. Road, Nagpur-10, India invites responses ("Proposals" / "Bids") to this RFP from eligible MSPs to be appointed as Managed Service Provider for procurement of Cloud services from MeitY Empaneled MSP for MRSAC Under MahaBHUMI Project.

Interested MSPs from MeitY empaneled cloud providers are advised to study this RFP document carefully before submitting their proposals in response to this RFP Document. Submission of a proposal in response to this RFP shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications.

The RFP can be downloaded from https://mahatenders.gov.in/nicgep/app any subsequent corrigendum / clarifications will be shared on the e-mail ids provided by the organizations / individuals who have purchased the RFP. The time, date and venue details related to the pre-bid meeting and proposal submission are mentioned in the Fact Sheet. Proposals must be received not later than time, date and venue mentioned in the Fact Sheet.

Proposals that are received after the deadline will not be considered. MSP will be selected under Quality and Cost based Selection (QCBS) criteria and procedures described in this RFP. To obtain first-hand information on the assignment, MSP is encouraged to attend the pre-bid meeting on the date and venue mentioned in the Fact Sheet. Attending the pre-bid meeting is optional.

Director

MRSAC, Nagpur

MSPs are advised to study this tender document carefully before submitting their proposals in response to the Tender Notice and also 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

This document has been circulated for limited circulation only, amongst the MeitY empaneled MSP for procurement of Cloud services for MRSAC Under MahaBHUMI Project. Information shared to the MSPs 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 (MRSAC), an autonomous body under Planning Department, Government of Maharashtra has issued this Request for Proposal (hereinafter referred to as "RFP") for Selection of MSP for procurement of Cloud services for MRSAC under MahaBHUMI Project for
   5 years for DC and DR 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 MSP(s) 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 MSP(s) with information to assist them in the formulation of their proposals.

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 MSP may require.

4. This RFP is not an agreement by and between MRSAC and the prospective MSPs 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 MSP is advised to consider the RFP document as per his understanding and capacity. The MSPs are also advised to do appropriate examination, enquiry and scrutiny of all aspects mentioned in the RFP document before bidding. MSPs 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. 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 MSP 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. This 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 MSP, 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 MSP for

participation in the Bidding Process) towards any MSP 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 MSP 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 website (https://mahatenders.gov.in/nicgep/app) and MRSAC website.

4 Fact Sheet

Sale of Tender Document	18-07-2024
Tender Inviting Authority	Maharashtra Remote Sensing Application Centre (MRSAC)
Name of Project Work	Request for Proposal for Selection of Managed Service Provider MSP for procurement of Cloud services to MRSAC under MahaBHUMI Project of Govt. of Maharashtra for DC and DR for 5 years
Tender / RFP Reference No.	RFP Number MRSAC/CLOUD/04/2024-25
Place of availability of Tender Documents (RFP)	https://mahatenders.gov.in/nicgep/app
Place of submission of Bids	https://mahatenders.gov.in/nicgep/app
Tender Document (RFP)	Request for Proposal Document
Tender Type (Open / Limited / EOI / Auction / Single)	Open
Tender Category (Service / Goods / Works)	Services
Type / Form of Contract (Work / Supply / Auction / Service / Buy / Empanelment / Sell)	Services
Re-bid submission allowed by the MSP (Yes / No)	Yes
Is Offline Submission Allowed (Yes / No)	No
Withdrawal Allowed (Yes / No)	Yes (on / before the last date and time of bid submission)
Is Multi Currency Allowed	No (Only Indian Rupees)
Date of release of RFP	18-07-2024
Payment Mode (Online / Offline)	Online
One time Procurement	Yes
Bid Validity days (180 / 120 / 90 / 60 / 30)	180 days
Location (Work / Services / Items / As per RFP)	As per RFP
Cost of Tender Document	A non-refundable fee of Rs. 25000/- to be paid online only. MSPs must enclose the receipt of same along with General cum Technical Bid.
Bid Security / Earnest Money Deposit (EMD)	Rs. 25, 00,000/- only. To be paid online or by submitting a Refundable & Irrevocable Bank Guarantee from any Scheduled Commercial Bank / Nationalized Bank drawn in favor of Director MRSAC, Nagpur valid for a period of minimum 180 days

Address to send Pre-bid Queries	Email ID: admn-mrsac@mrsac.gov.in Maharashtra Remote Sensing Application Centre (MRSAC), VNIT Campus, South Ambazari Road, Nagpur, Maharashtra – 440010
Nature of Bid Process	Two stage bidding Eligibility Criteria + Technical Bid Commercial Bid
Method of Selection	Quality and Cost based Selection (QCBS)
Last Date and Time for submission of Pre-Bid queries	25-07-2024 till 5:30 PM
Date of Pre-bid Meeting	26-07-2024 at 11:30 AM
Place of Pre-bid meeting	Maharashtra Remote Sensing Application Centre (MRSAC), VNIT Campus, South Ambazari Road, Nagpur, Maharashtra - 440010
Last date and time for Submission of Bids	20-08-2024
Opening of General cum Technical Bids uploaded on https://mahatenders.gov.in/nicgep/app	21-08-2024
Opening of Commercial Bids	To be communicated later
Name and Address of correspondence	Maharashtra Remote Sensing Application Centre (MRSAC), VNIT Campus, South Ambazari Road, Nagpur, Maharashtra - 440010

5 Introduction

5.1 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.

5.2 Project Background

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) – (MahaBHUMI Project). MRSAC is 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. 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 limit to) latest IT hardware / software / Cloud services.

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 this 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 host the production environment on the cloud.

5.3 Broad Objectives of MahaBHUMI Project

The objectives of this project are to ensure the following:

i. Providing easy, anywhere and anytime access to end users (both information & transactional) to ensure reliability, efficiency, transparency and accountability.

ii. Delivery to all user departments with Remote Sensing (RS) and Geographical Information System (GIS) services at state / district / taluka / town level in electronic form through state portals by using the MGDDS.

iii. RS and GIS applications to be hosted on Cloud 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.

5.4 MRSAC Requirements

Department intends to issue this tender document, to eligible entities, to participate in the competitive bidding for appointment of a vendor for providing Cloud Hosting & Managed Services initially for MRSAC and gradually for other requirements as and when required.

For this purpose, MRSAC invites proposals for appointing a Managed Service Provider (MSP) along with Cloud Service Provider (CSP) for activities mentioned under the Scope of Work in respect of procuring Cloud Services and Managed Services.

Managed Service Provider shall be solely liable to and responsible for all obligations towards the performance of works / services / adherence to SLAs under the contract and the cloud service provider shall be empanelled with MeitY for providing cloud services.

MRSAC currently hosts its production environment in On-premise data centre located at MRSAC, Nagpur. Through this tender, MRSAC intends to migrate the Production Environment to the Cloud for hosting GIS and Image applications.

5.5 Cloud hosting general requirements

i. Department requires the cloud service provider to extend its IT requirements as per demand. The cloud service provider should follow the below basic compliance requirement:

ii. MeitY has empaneled the Cloud Service offerings of MSPs in the form of Bouquet of Cloud Services.

iii. The cloud service provider should be listed on the https://eprocure.gov.in portal.

iv. CSP should be MeitY empaneled. The proposed data centre for hosting should be clearly mentioned and same must be mentioned on the https://meity.gov.in.

v. The cloud environment shall be hosted on Government Cloud Community (GCC) / Virtual private cloud (VPC) for hosting government client.

vi. MSP shall offer DR cloud services with their Data Centre location within India only. All the physical servers, storage, and other IT hardware from where cloud resources are provisioned for department must be within Indian Data Centre only. MSP shall ensure that department data resides within India only.

vii. All monitoring, provisioning, should be within India and 100% isolated from other regions outside India, if in case MSP has Global presence.

viii. The MSPs shall comply or meet any security requirements applicable to MSP published by the Government bodies such as CERT-IN, NCIIPC etc. at the time of bid submission. The MSP shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the MSPs and shall comply with the audit criteria defined by STQC.

ix. The DR Solution shall be on Active (DC) – Standby mode.

x. MSP to provide a primary site Data Centre (DC) and provide a Disaster Recovery (DR) setup in physically different zone other primary site Data Centre (DC) and MRSAC proposes to have Disaster Recovery to be setup up (50% of DC) considering given capacity as per BOQ and should execute all the operations smoothly in case of any disaster at primary site (DC). The Disaster Recovery site should be in different seismic zone than primary Data Centre.

xi. MSP to ensure that Drills be done half-yearly and for at least a period of 15 days. During DR drill, live operations to run from DR site with full load for a period of 15 days. MSP to provide MRSAC, all security components to factor as per the MeitY guidelines & relevant Indian IT act.

xii. All the components mentioned will follow Pay as you go pricing model on actual consumption

xiii. The department is not bound to avail all the services mentioned in the list

xiv. Data copy (download & upload) from MRSAC to DC and vice versa will be needed on a real-time, near-real-time and batch as needed.

xv. Bandwidth should be provided for regular data synchronization to DR site as per the RPO and RTO requirements at pre-defined intervals (daily or weekly)

xvi. The MSP should provide 64 VM (20 VMs required for GIS applications, 44 VMs for Open source and MIS applications), compute server, storage, network bandwidth from the CSP as Infrastructure as a service, managed services, security services. The proposed solution shall be hyperscale computing, extensible, highly configurable, secure, and very responsive and shall support integration and optimization including scale up and scale down of required services and solutions. The cloud should also provide upgradation as per future requirement by department.

The quantity and configuration of the service requested may vary in future, and the MSP needs to make the provision for accommodating the same.

Note: The MSP will ensure that all the licenses of proposed application / software, ESRI software, Hexagon, Apollo server, etc. procured for this project will be provided by MRSAC.

5.6 Responsibilities of MSP and CSP

5.6.1 <u>Responsibilities of MSP</u>

i. MSP shall be solely liable to and responsible for all obligations towards the performance of works / services / adherence to SLAs under the contract.

ii. MSP will be responsible for migrating to cloud and managing the cloud service offerings.

iii. The MSP shall be responsible for managing and controlling the underlying Cloud infrastructure including operating systems, storage, network, security, etc. and the deployed applications shall be managed and controlled by MRSAC.

iv. It is the responsibility of the MSP to monitor the cloud services (Resource Management, User Administration, Performance, and Service Levels.

v. Establishing point to point connectivity between MRSAC premise to Cloud DC and DR site

vi. Deploying new applications on Cloud, user administration, security administration, planning and implementation of Cloud Management and Monitoring Portal for complete infrastructure and services procured

vii. Monitoring & Reporting services

viii. Exit management and billing management.

ix. Compute Services: Provisioning, installation, Configuration, Commissioning / De-commissioning and Management of the Virtual Machines and provide MRSAC the access to the same via secured web browser / Command Line Interface

x. Storage Services: Provisioning of scalable storage capacity as per requirements of the MRSAC and availability of services

xi. Managed Database Services: Setting up, installation, configuration, management, upgradation and migration of Database Servers

xii. Network Services: Maintain and manage the required networks components for the Cloud Services

xiii. Security Services: Provisioning, Installation, Configuration, Management, Monitoring of Security Services as per the requirements of MRSAC.

xiv. Disaster Recovery Plan and Implementation: Setup and configuration of VMs, Storage, Network, Database, etc. at DR site meeting RPO and RTO requirements of the MRSAC.

xv. MSP shall be responsible for managing and controlling the underlying Cloud infrastructure including operating systems, storage, network, security, etc.

5.6.2 Responsibilities of CSP

i. Offer services in accordance with the Cloud Service Model proposed as per the RFP.

ii. Offer MRSAC with the elements such as facilities, data centers, network interfaces, processing, hypervisors, storage, and other fundamental computing resources where MRSAC is able to deploy and run Cloud Service Model.

iii. Ensure successful network connectivity is established between MRSAC location(s) and Cloud DC-DR site.

iv. Ensure the appropriate security controls for physical and logical security are in place at Cloud DC and DR

v. Ensure data is successfully replicated between the Cloud DC and Cloud DR and as per the required RPO specified by MRSAC.

vi. Ensure successful replication link is established between Cloud DC and DR site

6 Pre-Qualification

i. Pre-qualification Process

ii. MSPs are required to submit the Pre-Qualification documents in Techno-commercial bid to be uploaded online on https://mahatenders.gov.in/nicgep/app

iii. The MSPs Pre-Qualification Proposal in the bid document will be evaluated as per the requirements specified in the RFP and adopting the pre-qualification criteria spelt out in this RFP. The MSP is required to submit all required documentation in support of the pre-qualification criteria specified.

iv. The MSP shall meet all the mandatory compliance requirements. Failure in meeting the mandatory compliance requirements will result in disqualification of the MSP.

v. All the MSPs will be communicated of the results of evaluation of the pre-qualification bids.

vi. The Technical bids of those MSPs who qualify in the prequalification process only will be evaluated further against the technical bid evaluation criteria specified in the RFP and who do not qualify will strictly be rejected.

6.1 Pre-qualification Criteria for Managed Service Provider (MSP):

S. No	Pre-Qualification Criteria	MSP	Documents required substantiating pre- qualifying criteria
1.	The MSP 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. OR Limited Liability Partnership firm registered under Limited Liability Partnership Act, 2008.	Mandatory	Copy of Certificate of Incorporation / Registration Certificate
2.	The MSP should be single partner / firm registered in India. No consortium of firms is allowed.	Mandatory	Copy of Certificate of Incorporation / Registration Certificate
3.	The MSP should be in existence for minimum of 10 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.	Average annual turnover of the last three audited financial years (FY 2020-21, FY	Minimum INR 45 Crores	Audited Balance sheets and Profit & Loss account statements of the MSP for each

S. No	Pre-Qualification Criteria	MSP	Documents required substantiating pre- qualifying criteria
	2021-22, FY 2022-23) from IT / ITES / Cloud services		of the last three audited financial years FY 2020- 21, and FY 2021-22, FY 2022- 23 1. Certificate duly signed by Statutory Auditor of the MSP or Certified Chartered Accountant for average annual turnover from IT / ITES / Cloud services.
5.	The MSP must have a positive net worth in each of the last 3 financial years	Mandatory	Certificate duly signed by Statutory Auditor of the MSP or Certified Chartered Accountant specifying the net worth of the MSP.
6.	The MSP should possess the following valid certification as on bid submission date: ISO 9001, ISO 20000, ISO 27001	Mandatory	Copy of valid certificate issued by the competent authority, for ISO 9001, ISO 20000, ISO 27001 as on bid submission date
7.	The MSP, in last 5 years (as on bid submission date) should have undertaken at least One (1) Project of Cloud/ Private cloud* with project value of at least Rs. 20 Crore OR Two (2) projects of minimum value of 10 Crore each having scope of Application and Data Migration Services to Cloud/ Private Cloud (If two (2) projects then at least one project should be Cloud/ Private Cloud, setting up & hosting of IT infrastructure & systems at Cloud/ Private cloud) and providing managed services.	Mandatory	On Going Project + Invoice Copy or Work, order (WO) / Contract document(s) and 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.
8.	The MSP 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.
9.	The MSP must have valid Goods Tax registration in India & PAN card	Mandatory	Proof of valid Goods Tax Registration in India & Copy of PAN Card
10.	A Board Resolution or Power of Attorney, in the name of the person executing the bid, authorizing the signatory to sign on behalf	Mandatory	As per the format given in Annexure I, Point no. 15.1.3 of this document

S. No	Pre-Qualification Criteria	MSP	Documents required substantiating pre- qualifying criteria
	of the Bidding entity. The person issuing the Power of Attorney shall possess Board Resolution in his favour for granting such rights. In case of generic Board Resolution or Power of Attorney, the same shall be certified by Company Secretary.		

6.2 Pre-qualification Criteria for Cloud Service Provider (CSP):

Eligibility Criteria for the Cloud Service Provider (CSP)		
S. No	Pre-Qualification Criteria	Documents required substantiating pre- qualifying criteria
1.	The CSP should be registered under Companies Act, 1956 or as amended or an LLP firm / Partnership firm under Partnership Act 1932. The CSP should have an average annual turnover of INR 350 Crores for last three financial years (2021-22, 2022-23, 2023-24) and positive net worth as on 31st March 2024 or as on financial audit date of last financial year with at least 3 years of Operations in India as on bid submission date.	• Copy of Certification of Incorporation / Registration Certificate • Audited Balance sheet and Profit & Loss; for the last three financial years (2020-21, 2021-22, 2022-23) If Audited Balance Sheets and Profit & Loss account statements are not available for FY 2022 –23, then the SI may provide the Certificate duly signed by Statutory Auditor of the SI or Certified Chartered Accountant for average annual turnover • Certificate from the Statutory Auditor / Company Secretary on turnover details for the last three financial years (FY 2020-21, 2021-22, 2022-23) • Certificate from the Statutory Auditor / Company Secretary on positive net-worth for the last three financial years (2020-21, 2021-22, 2022-23)
2.	The CSP must be operating at least two (2) Cloud Solution site / disaster recovery site in India in different seismic zones at time of submission of the bid.	Self-certificate from the CSP mentioning the location details signed by authorized signatory of the CSP for this bid
3.	The CSP shall be MeitY's empaneled & STQC audited as per Ministry of Electronics and Information Technology (MeitY) as on bid submission date.	Valid Letter of Empanelment / Certificate of Empanelment from MeitY) including details on STQC audit status
4.	CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and / or privacy Trust Services principles such as SOC 1, SOC 2, SOC 3.	Copies of valid certificates (SOC1, SOC2 and SOC3) as on bid submission date

6.	SP should possess following mandatorily certifications: ISO 27001:2013 certification ISO / IEC 27017:2015-Code of practice for information security controls based on ISO / IEC 27002 for cloud services and Information technology. ISO 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds ISO 20000-1:2011 certification for Service Management System The Cloud should be on open source based technology to reduce dependency on licenses based solutions.	Copies of certificates valid as on bid submission date
7.	The CSP or proposed DC-DR facility should not have been blacklisted / debarred by any Central / State Government as on bid submission date	A self-certified letter by the authorized signatory of the MSP that the MSP has not been blacklisted by any Central / State Government (Central / State Government and Public Sector) or under a declaration of ineligibility for corrupt or fraudulent practices as of <bid submission date> must be submitted on original letter head of the MSP with signature and stamp
8.	The proposed Data Centre should be running Government community Cloud (GCC) or Virtual Private Cloud (VPC)	Valid copies of proof attested by authorized signatory
9.	CSP cloud platform must have ability to enable the below listed technology and OEM components on cloud Databases, Repositories and Data Stores: ✓ ArcGIS engine from ESRI ✓ Apollo Server ✓ MySQL Server 8 with GIS / image serving capabilities or above. ✓ PostgreSQL GIS / image serving capabilities)	Certificate and letter from authorized signatory on the letter head of CSP mentioning the compliance

Note:

i. Managed Service Provider (MSP) and Cloud Service Provider (CSP) may be a single entity. In such case, Managed Service Provider shall qualify for both the Criteria i.e., “Eligibility Criteria for the Managed Service Provider” and “Eligibility Criteria for the Cloud Service Provider”.

ii. Managed Service Provider (MSP) and Cloud Service Provider (CSP) may be different entity. In such case, Managed Service Provider shall qualify for “Eligibility Criteria for the Managed Service Provider” and Cloud Service Provider (proposed by MSP) shall qualify for “Eligibility Criteria for the Cloud Service Provider”.

iii. In any of the cases above, Managed Service Provider shall be solely liable to and responsible for all obligations towards the performance of works / services / adherence to SLAs under the contract.

iv. The MSP must quote solution with any one MeitY empaneled CSP only. The MSP must submit the Authorization letter from the CSP as part of Pre- qualification. Since the MSP will be evaluated on the proposed solution, they are not allowed to change the CSP post bid submission.

v. Supporting documents requested should be arranged / numbered in the same order as mentioned above.

vi. Failure to meet any of these criteria will disqualify the applicant and it will be eliminated from further process.

vii. The department reserves the right to verify and / or to evaluate the claims made under eligibility criteria and any decision in this regard shall be final, conclusive, and binding upon the company.

viii. All certificates or documents should also be self–attested and attached / bind together.

ix. If at a later stage it is found that applicant has provided false information or has wrongly certified the conditions stated in the eligibility criteria, the applicant shall be liable for legal action and / or cancellation of agreement / contract / license.

7 Instructions to MSP:

7.1 Purpose of Bid Document

This document provides information to enable the MSPs to understand the broad requirements to submit their "Bids".

7.2 Cost of Bid Document

The Cost of Tender document is INR 25000/- (Rupees Twenty-five thousand only) which shall be paid online.

7.3 Completeness of Bid Document

MSPs 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 MSP's risk and may result in rejection of the bid.

The MSP 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.

7.4 Proposal Preparation Cost

The MSP 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 MSP shall become the property of MRSAC and may be returned at its sole discretion.

7.5 Bid Cover Letters

Each MSP 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.

7.6 Power of Attorney

Each MSP 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 MSP during the full period of its validity. The original copy of the power of attorney document should be submitted to MRSAC before the bid submission deadline.

7.7 Pre-Bid Meeting

Department will host a Pre-Bid Meeting for queries (if any) raised by the prospective MSPs. The date, time and place of the meeting are given in this document. A maximum of 2 (two) representatives of MSP may attend the pre-bid meeting at their own cost. The purpose of the pre-bid meeting is to provide a forum to the

MSPs to clarify their doubts / seek clarification or additional information, necessary for them to submit their bid.

All enquiries from the MSPs relating to this Bid Document must be submitted to MRSAC at admn-mrsac@mrsac.gov.in.. These queries should also be emailed to queries should necessarily be submitted in the following format as a XLS & PDF Document:

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

Authorization letter in the name of the person attending pre-bid meeting needs to be submitted on the letterhead of the MSP during the pre-bid meeting in the format specified in this tender document.

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/nicgep/app

7.8 Amendments to Bid Document

At any time before the deadline for submission of bids, MRSAC may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective MSP, 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/nicgep/app

The MSPs 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 MSPs 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.

7.9 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 MSP's participation in this process may result in Department selecting the MSP 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.

7.10 Language of Bids

The Bids prepared by the MSP and all correspondence and documents relating to the bids exchanged by the MSP and Department, shall be written in English language, provided that any printed literature furnished by the MSP 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 MSP.

7.11 Bid Submission Format

The entire proposal shall be strictly as per the format specified in this Bid Document. MSP shall ensure that the bid documents are submitted in the respective folder online at https://mahatenders.gov.in/nicgep/app

7.12 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. MSPs shall furnish the required information on their technical and commercial proposals in the enclosed formats only. In case of any deviations in the format, bid will be liable for rejection.

iv. MSP 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 MSP may be verified with the original before issuance of Purchase Order. The successful MSP 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 (https://mahatenders.gov.in/nicgep/app).

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 MSP will have to submit additional document / clarification within 3 working days from the date of issue of the letter / mail seeking clarification / additional document.

ix. MRSAC 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) MSPs Tool Kit link (detailed Help documents, designed for MSPs) has been provided on e-Tendering website (https://mahatenders.gov.in/nicgep/app) 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

c) The tender notice / Tender document and clarifications / corrigendum (if any) shall be uploaded on e-Tendering website (https://mahatenders.gov.in/nicgep/app).

d) The date and time for online submission shall be communicated on the e-tendering website (https://mahatenders.gov.in/nicgep/app). 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 Upto 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 MSPs 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- MSPs will not be considered as forming part of their bid.

7.13 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/nicgep/app

ii) The MSPs participating first time for e-Tenders on e-tendering portal (https://mahatenders.gov.in/nicgep/app) will have to complete the Online Registration Process for the e-Tendering portal.

iii) All MSPs interested in participating in the online e-Tendering process are required to obtain Class II or Class III Digital Certificates. The tender should be prepared & submitted online using individual's digital signature certificate.

iv) The interested MSPs will have to make online payment of INR 25000/- (Non-refundable) as tender fee per tender at the time of entering online Bid Submission stage of the tender schedule.

7.14 Two Envelope Bid System

Complete bidding process will be online (e-Tendering) in two bid system. The MSP shall submit the bid proposal in 2 folders:

i) Pre-Qualification & Technical Folder

ii) Commercial Proposal

7.15 Supporting Documents for Bid

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

S.No	Type of Folder	Documents to be submitted
1	Pre-Qualification / Technical Folder	✓ Bid Cover Letter ✓ Power of attorney / board resolution to the authorized Signatory of the Bid ✓ Scanned copy of E.M.D. of INR 2500000/- and Online payment receipt of Tender Fee of INR 25000/- ✓ Particulars of the MSPs (in the given formats) ✓ Proof of Office address in Maharashtra ✓ Copy of Certificate of Incorporation / Registration Certificate ✓ Letter of authorization to attend bid opening (as per given format) ✓ Copy of the audited balance sheet of the company and Certificate from the Chartered Accountant clearly stating the net worth & Profit and Loss statement ✓ Self-declaration letter for not being blacklisted by Central / State Govt. as per given format. ✓ Proof of valid Goods & Service Tax Registration in India & Copy of PAN Card ✓ Copy of Work Order or Purchase Order ✓ Project Completion certificate from client and / or Go-live certificate from client, wherever applicable ✓ All other supporting documents as per Pre-qualification / Technical Qualification Criteria ✓ Manufacturer Authorization Form [as per given format] ✓ Self-declared Security Certificate (specifying no security related threats or non-compliances back doors, malware, virus etc.) pertaining to the supplied products. ✓ Technical Proposal ✓ Non-Disclosure Agreement (NDA)
2	Commercial Proposal Folder	✓ Commercial Proposal Cover Letter ✓ Commercial Bid (as per given format)

Note:

i. MSPs shall furnish the required information on their Pre-Qualification, technical and financial proposals in enclosed formats only.

ii. Any deviations in format may make the tender liable for rejection.

iii. Disclosure of Commercial information of the bid in Pre-Qualification /Technical Folder may be sufficient grounds for rejection of the bid.

7.16 Earnest Money Deposit (EMD) and Refund

MSPs are required to submit EMD online or in the form of Bank Guarantee of INR 25 Lakhs valid for 180 days from the dates of opening of bid, issued in favor of “DIRECTOR, MRSAC, NAGPUR” payable at NAGPUR from Nationalized Bank / Scheduled Bank in the pre- qualification folder. This Bank Guarantee must be submitted in the format specified in Bid Security Form. Offers made without Bid Security (in BG form) will be rejected. Bid shall be treated as invalid if scanned copies are not submitted online along with the bid. The MSP shall submit the BG physically in original form on or before the last date of bid submission at the following address:

The Director, Maharashtra Remote Sensing Application Center Department of Planning, Govt of Maharashtra, VNIT Campus, Ambazari Road, Nagpur-440010, Maharashtra

If such BG is not submitted physically as specified, the tender shall be treated as non-responsive and rejected. If a mismatch is found or the BG is not submitted physically within the time, the tender shall be treated as non-responsive and shall be rejected.

Unsuccessful MSP’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 MSP within 30 days, then MSP will not be liable to claim any interest on the extended period.

The successful MSP’s bid security will be discharged upon the MSP accepting the Purchase Order (issued by department) and furnishing the Security deposit / performance security in the form of performance bank guarantee. The bid security may be forfeited if an MSP withdraws its bid during the period of bid validity or in case of a successful MSP, if the MSP 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

7.17 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 MSP 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 does not constitute a material deviation according to Department.

The evaluation will be a 3-stage process:

i. Pre-qualification evaluation of all MSPs

ii. Technical Evaluation of MSPs who qualified pre-qualification stage

iii. Commercial Evaluation of MSPs who qualified technical evaluation stage

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

7.18 Opening of Bid

All the Bids will be received online the deadline shall be opened at the date, place and time mentioned in this tender document. Once the bids are opened, each bid will be checked for pre-qualification criteria.

7.19 Evaluation of Technical Bids

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

The EC may require verbal / written clarifications from the MSPs to clarify ambiguities and uncertainties arising out of the evaluation of the Bid documents. MSP 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 13.3.2 "Checklist for the documents to be submitted".

The MSPs are required to fill up technical specification Compliance Table, as per Annexures. Non- Compliance, if any, should be brought out very clearly. If MSP 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) MSPs, who attain total technical score of 70 (Seventy) or more, will qualify for the evaluation of commercial bids.

iii) The commercial bids of MSPs who do not qualify technically shall not be opened.

iv) The committee shall indicate to all the MSPs the results of the technical evaluation through online. The technical scores of the MSPs will be announced prior to the opening of the commercial bids.

v) The names of the technically qualified MSPs will be uploaded on the website (https://mahatenders.gov.in/nicgep/app) on the given date and subsequently commercial bids of the qualified MSPs will be downloaded for further consideration.

7.20 Notifications of Award and Signing of Contract

Prior to the expiration of the period of proposal validity, the MSP will be notified in writing or by email that its proposal has been accepted. MRSAC shall facilitate signing of the contract after the notification of award. However, it is to be noted that the date of commencement of the project and all contractual obligations shall commence from the date of issuance of Purchase Order / Letter of Acceptance, whichever is earlier. All reference timelines as regards the execution of the project and the payments to the MSP shall be consideredas beginning from the date of issuance of the Purchase Order / Letter of Acceptance, whichever is earlier. The notification of award (Purchase Order / LOA) will constitute the formation of the Contract. Upon the MSP executing the contract with MRSAC, it will promptly notify each unsuccessful MSP and return their EMDs. After issuance of Purchase Order / LOA the MSP shall sign the Contract as per the draft contract format given in Section 12.

7.21 Failure to agree with the Terms & Conditions of the Bid Document / Contract:

Failure of the MSP to agree with the Terms & Conditions of the Bid Document / Contract shall constitute sufficient grounds for the annulment of the award of contract and seizure of EMD amount. The contract may be awarded to the next most responsive bid of other MSP.

7.22 Terms and Conditions of the Tender

MSP is required to refer to the Draft Contract Agreement, at Section 12 in this RFP Document, for all the terms and conditions (including project timelines) to be adhered by the successful MSP during Project Implementation and Post implementation period.

8 Scope of Work

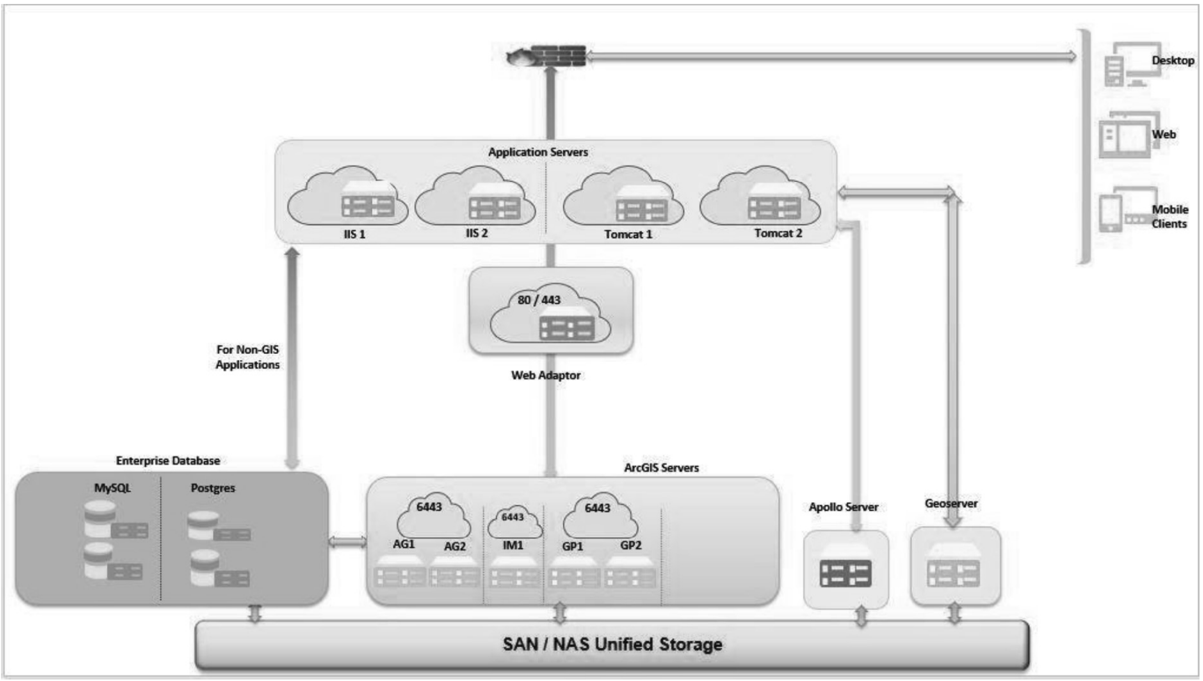
Maharashtra Remote Sensing Application Centre (MRSAC) was established in September 1988 at Nagpur as an autonomous organization under the administrative control of department of planning, Govt. of Maharashtra. Today, MRSAC is one of the well-established Centre. With full support of Govt. of Maharashtra, 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 existing On-premise 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 of GIS applications on Cloud through this RFP while retaining the development, staging and maintenance environment On Premise.

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.

The details of the current functionalities of the applications are stated below:



i. <u>Remote Sensing and GIS Based Mapping for Water Supply and Sanitation (WSS) using High Resolution Satellite Data for Maharashtra state</u>

a) The web-based management information system has been developed as a decision support tool for daily operation and maintenance of water supply schemes.

b) The portal is designed for viewing the various drinking water supply schemes and its related assets, catering the need of drinking water to all villages / habitations pertaining to Maharashtra State.

c) The other thematic and administrative layers in RS & GIS domain can be overlaid for better visual perception to decision / policy makers.

d) The WEB based geospatial technology is used for various management, dashboard visualization and decision analytics.

e) Satellite Imageries are always available in the backdrop to provide a near to site feeling for the decision makers.

f) This facilitates the simulation of the decision as taken from the field after verification.

ii. Mapping and Web Based Allocation Analysis of School using Geospatial technology

a) GIS mapping of schools using mobile application with screen shot facility.

b) Web based buffer analysis on primary school locations and existing habitations / settlements.

c) Generating the template containing buffer layers, school location, base layers and statistics.

d) School routing facility to find out distance between school location and habitation / settlement by giving UDISE code of school.

e) Search school by name, UDISE code and latitude and longitude.

f) Depiction of 13321 schools, having enrolment of students below 20.

g) Printing facility to provide district / taluka wise school location maps along with habitation / settlement locations.

h) Statistics and reporting

iii. Development of Geoportal for Maharashtra State Warehousing Corporation

a) To Convert CAD drawings of Layout Plans of 191 MSWC owned warehouse in to layers under GIS environment and generate Warehouse layout map in GIS environment with standard code and topology.

b) Geo-reference of Layout Plans of 191 MSWC warehouse using High Resolution Satellite Data.

c) GIS data creation on Warehouse of MSWC and other Govt. Departments based on inputs provided by MSWC.

d) To create facility for online route analysis & buffer from given location to Warehouse on geoportal which enable to locate nearest MSWC warehouse / godowns and details of warehouse in the radius of 10 km, 20 km, 30 Km, 50 km & also provide the infrastructure information pertaining to State / National Highway, nearest APMC centre name, nearest Railway station, nearest Police station and other important information within its periphery.

e) Mobile Application to daily capture data of vacant space available in warehouses other than the MSWC owned warehouses, location of procurement centres, and Mandi and depict on dashboard.

f) Integration of SAP data with GIS data for depicting the availability of current vacant space in the warehouses.

g) Development of Geoportal for MSWC.

iv. AMC Consumer Feedback Portal

a) GIS department of Akola Municipal Corporation approached MRSAC, Nagpur for development of "AMC Consumer Feedback Portal", for getting feedback from citizens regarding work done for Road, Sewerage, Culvert, etc within the limits of Akola Municipal Corporation (AMC). The main objectives are:

b) Design and development of web-based portal for getting feedback about the works carried out under Akola Municipal Corporation area for Road, Sewerage, Culvert, Electric pole, Handpump, Sub Pump, etc.

c) Development of dashboard for administrator of Akola Municipal Corporation and generate various types of reports.

v. Implementation of Integrated Enterprise Geographical Information System (GIS) for CIDCO

The Integrated Enterprise Geospatial Information System for City & Industrial Development Corporation of Maharashtra Ltd. (CIDCO) specifically covers Navi Mumbai area (a35pprox.. 344 sq km) in the Phase-I of the project. Out of 344 sq km. of Navi Mumbai Notified Area' about 114 sq km area comprises of other Planning Authorities such as NMMC' Panvel Municipal Council, Uran Municipal Council, MIDC and JNPT' Remaining about 230 sq. km. area is being administered by ClDCO. MRSAC shall digitize the entire 344 sq. km of Navi Mumbai pertaining to the cadastral and infrastructure layers using latest satellite images having regard to base map(s) available with CIDCO. Similarly, MRSAC shall carry out detailed mapping for 230 sq km area using the maps of Lands, Planning, Transportation, and Engineering Departments (all infrastructure / utilities etc.) of CIDCO.

Additional Functional Requirements

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 web portal development, mobile apps development with geotagging and geofencing capabilities, server installation, server maintenance, web portal migration, training the field officers, etc. Following are some of the departments and its Decision Support systems containing web portals and mobile apps:

- Agriculture
  a) MahaAgritech
  b) MahaMADAT (Drought)
  c) Warehouse Mapping
- Water Resources
  a) Jalyukt Shivar
  b) WSSD
  c) GSDA
  d) NHP-DSS
  e) WRD
  f) MTS
  g) GMD
  h) IWMP
- Relief & Rehabilitation
  a) E-Panchnama

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

Recently, 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.

The broad project scope requires a single service provider (MSP) to manage services for cloud Infrastructure. The department intends to procure the 'Cloud Hosting & Managed Services' for the business applications. The shortlisted MSP shall provide the Cloud Hosting & Complete Managed Services through this bidding process for the period of <03> years and the department reserves the right to extend the services for another <02> years based on the satisfactory performance.

The proposed solution shall be scalable, extensible, highly configurable, secure, and very responsive and shall support integration and optimization including scale up and scale down of required services and solutions (existing legacy and acquired in future), designed for or used by the department.

The broader requirements are mentioned below –

a) Cloud Infrastructure for Application Hosting (DC and DR).

b) End to End Managed Service

c) Application Migration from existing cloud

d) Optional Rate Card

8.1 Detailed scope of work

8.1.1 One-time integration Services for Provisioning and Validation of Secure Infrastructure

i. Establishing Cloud Service Provider (CSP) accounts

ii. Establishing the security and compliance framework and creating the security control design

iii. Network infrastructure Design and Provisioning

iv. IAM (identity and access management) based roles and policies for CSP services

v. Complete infrastructure configuration for virtual networks.

vi. Configure subnets, security group rules, network access control list, route table rules

vii. Configure connectivity for inbound and outbound access

viii. Application infrastructure provisioning

  a) Provision of production servers according to specifications

  b) Provision Database instance on the production servers

  c) Configure security for all provisioned servers

  d) Migration of the applications to the cloud infrastructures

  e) Support Application Setup, Testing and Production Deployment

  f) Provide infrastructure troubleshooting assistance during functional testing

  g) Support production deployment of applications and go-live activities

8.1.2 Ongoing infrastructure Managed Services (For the period of Contract)

i. **Remote infrastructure Monitoring**

a) Daily remote monitoring of all production instances in-scope

b) Monitor storage / space issues and manage any capacity issues

c) Configure and manage alarm notification list

d) Set-up and configure CSP audit trail, application and infrastructure monitoring

e) Configure connectivity for inbound and outbound access

f) Support Customer in creation and management of DNS records

g) Management of static lP allocation management

h) Gateway Management (CSP to on premise)

i) Management of Security Groups (Creation / Editing / Management)

ii. **Backup and Restore**

a) Determine / adhere to the appropriate backup requirement

iii. **Patching**

a) Update and patch all systems in a timely and secure manner including OS updates / upgrades.

b) implement patches as early as practical after the release

c) Patches should be applied with minimal disruption to production operations

d) Test and apply non-critical vendor software patches according to an agreed upon schedule

e) Perform regular maintenance of the environment, addressing event log errors and warnings

iv. **Incident Management**

a) Monitor the overall health of the infrastructure resources and handle the daily activities of investigating and resolving incidents.

b) Propose incident / Problem workflow, escalation, communication and reporting processes that support the Service Level Requirements

c) Troubleshoot and triage tickets using available tools and knowledge bases

d) Manage entire incident / Problem resolution lifecycle, including detection, diagnosis, progress reporting, repair and recovery, documentation and knowledge base updates

e) Record resolution in the ticketing system

f) Ensure incident Resolution activities conform to defined Change Control procedures

g) Track and report monthly recurring incidents, problems and failures and communicate associated consequences to MRSAC.

h) Recommend solutions to MRSAC to address trends, recurring Incidents, problems or failures

i) Review and approve solutions to address trends, recurring incidents, problems or failures

j) Notify stakeholders of the incident with an Estimated Time of Arrival (ETA) for resolution

v. **Security and Access Management**

a) Protect information assets and keep CSP infrastructure secure.

b) Setup anti-malware protection, intrusion detection, and intrusion prevention systems \

c) Manage security policies and quickly respond to any intrusion

d) Configure CSP security capabilities and best practices, such as ldentity and Access Management (lAM) roles and virtual firewall security

vi. **Cost Management**

a) Provide a monthly summary of key performance metrics, including operational activities, events and their respective impact, as well as recommendations to optimize platform usage and optimize cost so as to get the most out of CSP investment**.**

vii. **Knowledge Management**

a) Document procedures manual, run book, operations and administration procedures that meet requirements and adhere to defined policies

b) Operational reporting

c) Provide monthly status reviews including reporting, depicting performance against each service level requirement as below

d) Utilization report (Resource usage report)

e) Incident / Change reports

f) Ticketing reports

g) Cost reports

h) Security reports (logins, intrusion, denial of service, DDOS and other anomalies). Provide periodic status reviews to MRSAC to discuss incident activity, enhancement work (including backlog and new requests), planning and issue resolution

8.1.3 Express Connectivity between Cloud Service Zone and MRSAC Nagpur

Assured 24 / 7 full redundant express connectivity between cloud active zone (DC & DR) and MRSAC Nagpur for both point to point (100 Mbps) and Internet lease line.

8.1.4 The application software (ESRI, HEXAGON), the necessary licenses for deploying MahaBHUMI Project applications ecosystem comprising of the above work streams will be provided by MRSAC. Any additional licenses pertaining to Databases, and Operating systems (Native / external) will be provided by the MSP. The cost of procurement of additional licenses should be included in the financial bid.

8.1.5 The CSP, MSP, MRSAC and its developers shall be responsible for developing and provisioning appropriate solution components for enabling integration through API from the proposed cloud setup of MahaBHUMI Project to ^{3r}d party applications as per the requirement and at required frequencies.

8.1.6 The MSP shall maintain DC and DR for the required infrastructure adhering to all measures to ensure seamless data recover.

8.2 Operational Acceptance and Maintenance & Support of Cloud

i. Operational Acceptance shall commence once the system is commissioned for a period of maximum 30 days.

ii. Operational Acceptance will only be provided after cloud resources have been provisioned.

iii. The MSP will have to facilitate the Operational Acceptance Tests. Operational acceptance tests will be performed by MRSAC and the appointed MSP; however, MSP will have to facilitate Operation Acceptance during commissioning of the system (or subsystem[s]), to ascertain whether the system (or major component or Subsystem[s]) conforms to the scope of work. The MSP will have to facilitate the testing of application from MRSAC users during the Operational Acceptance. Necessary support shall be provided by the MSP.

iv. After the Operational Acceptance has completed, the MSP may give a notice to MRSAC requesting the issue of an Operational Acceptance Certificate.

v. MRSAC will Issue an Operational Acceptance Certificate OR Notify the MSP of any deficiencies or other reason for the failure of the Operational Acceptance Tests

vi. Once deficiencies have been addressed, the MSP shall again notify MRSAC, and MRSAC, with the full cooperation of the MSP, shall use all reasonable endeavours to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the MSP shall notify MRSAC of its request for Operational Acceptance, MRSAC shall then issue to the service provider the Operational Acceptance, or shall notify MSP of further deficiencies, or other reasons for the failure of the Operational Acceptance Test.

vii. The MSP's responsibility shall be as per the responsibility matrix with respect to 24*7*365 days support for MRSAC Cloud infrastructure for 05 years from the date of issuance of operational acceptance by MRSAC. The maintenance and support will include following activities -

   a. Compliance process to the defined international standards and security guidelines such as ISO 27001, ISO 20000:1, for maintaining operations of cloud and ensuring privacy of MRSAC data.

   b. Ensuring Uptime and utilization of the cloud resources as per SLA's defined in this RFP.

viii. In the event of a disaster at DC site, activation of services from the DR site is the responsibility of MSP. It shall develop appropriate policy, checklists in line with ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate DR site. DR drills needs to be performed by the MSP half yearly to check disaster preparedness MSP shall support the application vendor through all these activities. The MSP will ensure that The DC & DR sites shall be separated by a minimum distance of 100 kilometres as per MeitY guidelines.

ix. The MSP shall conduct vulnerability and penetration test (from a third-party testing agency which may be CERT-IN empaneled appointed by MRSAC) on the Cloud facility every 6 months in consultation with MRSAC and reports should be shared with MRSAC. The MSP needs to update the system in response to any adverse findings in the report, without any additional cost to MRSAC.

x. Upgrades - Any required version / Software / Hardware upgrades, patch management etc. at the Cloud Site will be supported by the MSP for the entire contract period at no extra cost to MRSAC.

xi. MSP is required to provision additional VM's when the utilization exceeds 80%.

xii. On expiration / termination of the contract, MSP to handover complete data in the desired format to MRSAC which can be easily accessible and retrievable. The MSP has to provide full support for migrating data from the primary DC site to another site if required in the future.

xiii. MIS Reports - MSP shall submit the reports on a regular basis in a mutually decided format. The MSP shall workout the formats for the MIS reports and get these approved by the MRSAC after awarded the contract. The following is only an indicative list of MIS reports that may be submitted to MRSAC:

   a. Daily reports

      1. Summary of resolved unresolved and escalated issues / complaints

2. Log of backup and restoration undertaken

b. Weekly Reports

1. Summary of issues / complaints logged with the OEMs.
2. Summary of changes undertaken in the Cloud environment
3. OS and database patch update status

c. Monthly Reports

1. Component wise resource availability and resource utilization
2. Consolidated SLA / Non- conformance report.
3. Summary of component wise uptime.
4. Log of preventive / scheduled maintenance undertaken
5. Log of break-fix maintenance undertaken
6. All relevant reports required for calculation of SLAs

d. Quarterly Reports

1. Consolidated component-wise availability and resource utilization
2. All relevant reports required for calculation of SLAs
3. The MIS reports shall be in-line with the SLAs

xiv. Provisioning Cloud services for additional quantities at proposed rate

a) Annexure II specifies, quantities and compute for IT Infrastructure components for availing cloud services.

b) Based on future requirements, MRSAC is likely to purchase additional quantities of cloud service covered in this RFP.

c) The rates offered for cloud services must be valid for entire contract / project duration. No variation in these quoted rates shall be allowed during this period.

d) MRSAC will have liberty to order additional cloud service items, at the rates offered in the commercial bid.

e) MRSAC reserves the right to scale down and scale up the IT infrastructure. The payment would be made only on the actual usage of the IT infrastructure as per the rates provided by the MSP in their Commercials.

8.3 Resource Management and Service Provisioning:

i. Cloud service provider should enable MRSAC to provision cloud resources through self service provisioning portal.

ii. MSP should enable MRSAC to provision cloud resources from application programming interface (API).

iii. The user admin portal should be accessible via secure method using SSL certificate.

iv. MSP should enable MRSAC to provision additional resources from provisioning portal as and when require.

v. MSP should enable MRSAC to take snapshot of virtual machines from provisioning portal.

vi. MSP should enable MRSAC to size virtual machine and select require operating system when provisioning any virtual machines.

vii. MSP should enable MRSAC to predict his billing of resources before provisioning any cloud resources.

viii. MSP should enable MRSAC to set threshold of cloud resources of all types of scalabilities.

ix. MSP should enable MRSAC to provision all additional storages require for cloud services.

x. MSP should enable MRSAC to provision any kind of resources either static or elastic resources.

xi. MSP should enable MRSAC to take console of cloud virtual machines from portal to perform any operations.

xii. MRSAC should get list of all cloud resources from provisioning portal

xiii. MSP should enable MRSAC to set the scaling parameters like in case of horizontal scaling:

1) to set percentage / quantity of RAM consumption to trigger new virtual machines.

2) to set percentage / quantity of CPU consumption to trigger new virtual machines.

3) to set percentage / quantity of network bandwidth to trigger new virtual machines

xiv. MSP should enable MRSAC to set port on which horizontal scaling will work.

xv. MSP should enable MRSAC to set minimum and maximum number of virtual machines which will be automatically provisioned as part of horizontal scaling to handle spike in load.

xvi. The cloud virtual machine created by portal should have at-least two virtual NIC cards. One NIC card should be used for internet traffic while other should be used for internal service traffic.

xvii. The Solution should provide a simple to use intuitive Web and experience for DC cloud administrator and user departments

xviii. The Solution should have self-service capabilities to allow Users Departments to log service requests – in DC.

xix. The Solution should be able to offer choice of various Service offering on multiple hypervisors (such as Hyper-V, VMWare, KVM) with an option to select multi operating systems such as Windows server 2019, RHEL / SUSE Linux, etc., VLAN, Storage and quickly compute associated price for the same as well as shows the deduction for overall Tenant approved infrastructure Quota.

xx. The Solution should offer Service catalogue listing availability of Cloud infrastructure like Virtual Machines, Physical Machines, Applications, Common Services offered by State Private cloud.

xxi. The Solution should automate provisioning of new and changes to existing infrastructure (Virtual, Physical, Application or Common Services) with approvals.

xxii. The Solution should allow creation of library hosting various Operating System, Databases and middleware that can be selected while creating new virtual servers

xxiii. The Solution should track ownership and utilization of virtual machines, Physical machines, and common services.

xxiv. The Solution should have the ability to manage virtual assets across the major multiple virtualization platforms (Microsoft, VMware, Xen, etc.)

xxv. The solution should be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool.

xxvi. The solution should offer usage report by tenant, by region, or by virtual machine reporting usage of memory consumption, CPU consumption, disk consumption

xxvii. The solution should allow the users to schedule a service creation request in a future date / time; the solution should check if a request scheduled for a future time can be fulfilled and reject the request in case of projected resources shortage or accept the request and reserve the resources for that request.

xxviii. The Solution should have web-based interface for administration.

xxix. The Solution should have the ability generate customize report as well as the native ability to export to common formats.

8.4 User Administration and Management:

i. Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks. (Only relevant if IAM is getting implemented)

ii. Administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles they associated with the user account.

iii. Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it.

iv. For analysis purpose the Dashboard should contain following information

a. Number of requests to web server.

b. Number of attacks.

c. Number of Attackers.

d. Types of error messages and on. Of error messages sent to the users.

e. Total Bytes sent during transaction

9 Technical Requirements:

9.1 Requirement for Cloud:

TABLE 1 BILL OF MATERIAL

Compute node with standard storage					
S No.	Items	vCPU	Memory RAM (GB)	OS Size SSD (GB)	UoM
1.	Windows Server 64 bit	8 Core	16	500	Per VM
2.	Windows Server 64 bit	8 Core	32	500	Per VM
3.	Windows Server 64 bit	8 Core	64	500	Per VM
4.	Windows Server 64 bit	16 Core	32	500	Per VM
5.	Windows Server 64 bit	16 Core	64	500	Per VM
6.	Windows Server 64 bit	16 Core	128	500	Per VM
7.	Windows Server 64 bit	32 Core	64	500	Per VM
8.	Windows Server 64 bit	32 Core	128	500	Per VM
9.	Windows Server 64 bit	32 Core	256	500	Per VM
10.	Windows Server 64 bit	64 Core	128	500	Per VM
11.	Windows Server 64 bit	64 Core	256	500	Per VM
12.	Windows Server 64 bit	64 Core	512	500	Per VM
Compute node with NVMe storage for OS					
S No.	Items	vCPU	Memory RAM (GB)	OS Size SSD (GB)	UoM
13.	Windows Server 64 bit	8 Core	16	500	Per VM
14.	Windows Server 64 bit	8 Core	32	500	Per VM
15.	Windows Server 64 bit	8 Core	64	500	Per VM
16.	Windows Server 64 bit	16 Core	32	500	Per VM
17.	Windows Server 64 bit	16 Core	64	500	Per VM
18.	Windows Server 64 bit	16 Core	128	500	Per VM
19.	Windows Server 64 bit	32 Core	64	500	Per VM
20.	Windows Server 64 bit	32 Core	128	500	Per VM
21.	Windows Server 64 bit	32 Core	256	500	Per VM
22.	Windows Server 64 bit	64 Core	128	500	Per VM

23.	Windows Server 64 bit	64 Core	256	500	Per VM
24.	Windows Server 64 bit	64 Core	512	500	Per VM

Storage Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
25.	Disk Storage (Block)	Primary storage for data	Per 1 TB
26.	Disk Storage (File)	Primary storage for data	Per 1 TB
27.	NVMe SSD Storage	NVMe storage with 50K IOPS	Per 1 TB
28.	Backup Storage	Backup Storage in Object Store	Per 1 TB

Network Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
29.	Virtual Firewall 1Gbps throughput + IPS +IDS features-VM level and Subnet level	Allow / Deny inbound & outbound traffic	Per Firewall
30.	Virtual Server Load Balancer 1Gbps throughput	Load balance applications and for failover	Per VLB
31.	Virtual WAF 1Gbps throughput	Dedicated WAF to protect web application from external vulnerabilities	Per Gbps
32.	Content Delivery Network	For copying data to multiple locations	Per GB
33.	Unmetered Internet Bandwidth – Primary Site (independent of down / up data size)	100 Mbps	Per 10 Mbps
34.	Internet Bandwidth – DRs	Internet bandwidth of 50 Mb/ s	Per 10 Mbps
35.	Site to Site VPN	VPN connections	Per connection
36.	Point to Site VPN	VPN connections	Per connection
37.	Public IP v4	To provide IP address for Applications.	Package of 16
38.	Networking Monitoring Dashboard / Monitoring tool - Visualize CPU, Server, Memory, Disk, Utilization, Raise alarm for threshold bridge	Visualising CPU, Server, Memory, Disk etc	Contract period (60 months)
39.	Caching Services	Caching	Per GB

Security Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)

40.	SIEM solution with log retention 90 days	To provide real-time analysis of security alerts generated by applications and network hardware.	Per 500 EPS
41.	DDOS	Blocking and absorbing malicious spikes in network traffic and application usage caused by DDoS attacks, while allowing legitimate traffic to flow unimpeded.	Per 100 Mbps
42.	Domain SSL wildcard	Public key certificate which can be used with multiple sub-domains of a domain. The principal use is for securing web sites with HTTPS.	Per domain
43.	Anti-Virus with centralized Management	To protect your business systems from viruses and other threats.	Per VM
Other Components			
S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
44.	Memory	8 GB	Per 8 GB
45.	HDD	Hard disk	Per 5GB
46.	NVMe SSD	NVMe SSD	Per 5GB
47.	vCPU	No of cores	Per vCPU
48.	Postgres Enterprise license with post GIS	Managed DB services	Per month

9.2 General Requirement

S.No.	General Requirement	Compliance (Yes / No)
1.	Ability to handle Raster and vector data	
2.	Ability to capture, store, retrieve and render on web application – Raster and vector files of the size ~ 2 TB	
3.	Ability to provide Postgres database instances on demand to handle the vector and image data pertaining to the whole of Maharashtra.	
4.	Ability to handle 100 users concurrently	
5.	Ability to load Apache Tomcat / IIS Server to handle the web application via secure method using SSL certificate	
6.	Ability to load and run ArcGIS Server / Geoserver, Apollo Server etc. on cloud.	
7.	Ability to handle WMS, WFS, WCS etc. web services.	
8.	Ability to load Java, Java Script, .Net, etc. based applications	
9.	Ability to enable information, services and data exchange with external applications through open API integration	

S.No.	General Requirement	Compliance (Yes / No)
10.	Proposed solution should be capable to employ full-service, closed-loop automation for IT operating system and infrastructure compliance and vulnerable.	
11.	Solution must provide auto scale out and scale in so that in case of increase in utilization additional VMs should automatically be created with all networks, security and load balancing assigned. All components needed to achieve this including but not limited to cloud portal, orchestration, virtualization, overlay network, security and load balancer should be provided and integrated to achieve full automation.	
12.	MRSAC should be able to create, delete, shutdown, reboot virtual machines from provisioning portal and RDP	

9.3 Compute Requirement:

S.No.	Compute requirements for standard and NVMe Storage	Compliance (Yes / No)
1.	The MSP shall do provisioning for required computing resources for hosting of all the required IT applications as listed.	
2.	Virtual Machines shall be required to run the variety of workloads such as compute-intensive workload, memory-intensive workload, general-purpose workload, etc.	
3.	The MSP shall deploy VMs on Server-Hardware having 1:2 Physical Core to vCPU ratio	
4.	CPU (Central Processing Unit) shall be provided with a minimum equivalent processor speed of 2.4GHz. The CPU shall support 64-bit operations. VMs shall support Intel, AMD based processor	
5.	The Cloud virtual machine provided by MSP should be provisioned on redundant physical infrastructure.	
6.	The cloud virtual machines should be auto scalable in terms of RAM and CPU automatically without reboot.	
7.	MRSAC should be able to provision cloud virtual machine of any operating system like Linux, Windows, etc.	
8.	MSP should clearly define policies to handle data in transit and at rest.	
9.	MSP should not delete any data at the end of agreement without consent from MRSAC.	
10.	MSP should provide facility to make template from virtual machines.	
11.	MSP should enable MRSAC to select configuration of cloud virtual machine-like custom RAM, CPU, and disk.	
12.	MSP should enable MRSAC to add either block storage volume or file level storage block to cloud VM from provisioning portal.	
13.	MSP should give provision to make clone of cloud virtual machine of MRSAC from provisioning portal.	
14.	MSP should make provision so that MRSAC can add any virtual machine as part of scalable infrastructure.	
15.	MSP should have provision to live migration of virtual machine in case of any failure to another virtual machine or physical servers as required.	
16.	MSP should provide facility to use different types of disks like SAS, SSD based on type of application.	
17.	MSP should provide network information of cloud virtual resources.	

S.No.	Compute requirements for standard and NVMe Storage	Compliance (Yes / No)
18.	MSP should offer provision to monitor latency to cloud virtual devices from its datacenter or MRSAC should be able to set monitoring of latency to cloud VMs from outside the datacenter.	
19.	MSP must offer provision to monitor network uptime of each cloud virtual machine	

9.4 Storage Requirement

S.No.	Storage Requirements General	Compliance (Yes / No)
1.	MSP should provide scalable, dynamic and redundant storage.	
2.	MSP should offer provision from self-provisioning portal to add more storage as and when required by MRSAC.	
3.	MSP should clearly differentiate its storage offering based on IOPS. There should be standards IOPS offering per GB and high-performance disk offering for OLTP kind of workload. MSP should delivery minimum 3000 IOPS per TB for OLTP load for NON OLTP load should be minimum 1000 IOPS per TB.	
4.	MSP should have block disk offering as well as file / object disk offering to address different kind of MRSAC needs.	
5.	MSP should allow minimum space of 1 GB to be provisioned by MRSAC from self-service provisioning portal.	
6.	MSP must give provision to attach new disk block to any cloud VM MRSAC needs from self-service portal	
7.	Cloud provider should offer a highly scalable, high-performance storage.	

S.No.	Block Storage Requirements	Compliance (Yes / No)
1.	MSP should offer persistent block level storage volumes for use with compute instances.	
2.	Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies.	
3.	Cloud service should support the needs of I / O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I / O throughput.	
4.	Cloud service should support encryption of data on volumes, disk I / O, and snapshots using industry standard AES-256 cryptographic algorithm.	
5.	Cloud service should support encryption using customer managed keys.	
6.	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.	
7.	Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data center migration, and disaster recovery.	
8.	Cloud service should support adding more than one compute instance to a single storage volume in R / W mode so that many users can access and share a common data source.	

S.No.	Block Storage Requirements	Compliance (Yes / No)
9.	Cloud service should support a baseline IOPS / GB and maintain it consistently at scale.	

S.No.	File Storage Requirements	Compliance (Yes / No)
1.	MSP should offer a simple scalable file storage service to use with compute instances in the cloud.	
2.	MSP should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads.	
3.	Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections.	
4.	Cloud service should support consistent low latency performance between 5-15 MS at any scale.	
5.	Cloud service should support scalable IOPS and throughput performance at any scale.	
6.	Cloud service should support thousands of instances so that many users can access and share a common data source.	
7.	Cloud service should automatically scale up or down as files are added or removed without disrupting applications.	
8.	Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple datacenters.	
9.	Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).	

S.No.	Backup and Restore Service	Compliance (Yes / No)
1.	MSP shall provide backup solution, covering but not limited to daily, weekly, monthly, quarterly, and annual backup functions (full volume and incremental) for data and software maintained on the servers and storage systems using Enterprise Backup Solution.	
2.	MSP shall cover (not limited to) Backup & Restoration of VM images, Operating System, Applications, Databases and File system etc.	
3.	MSP shall Configure, schedule, monitor and manage backups of all the data including but not limited to files, images, and databases as per the policy / procedure / plan finalized by department.	
4.	MSP shall also perform Administration, tuning, optimization, planning, maintenance, and operations management for backup and restore.	
5.	MSP should propose cloud native solution or use a SaaS based / Third Party software deployed on VM based backup software.	
6.	The Long-Term Storage should have an option of enforcing WORM (Write Once, Read Many) policy for section of data that requires the same.	
7.	MSP shall Provide and install additional infrastructure capacity for backup and restore.	
8.	MSP shall perform restoration testing biannually with the permission of department.	
9.	MSP must ensure integrity of the data returned during a restore by verifying the block data read with a check sum of the data.	

<table>
<tr><th>S.No.</th><th>Backup and Restore Service</th><th>Compliance (Yes / No)</th></tr>
<tr><td>10.</td><td>MSP shall ensure prompt execution of on-demand backups & restoration of volumes, files and database applications whenever required.</td><td></td></tr>
<tr><td>11.</td><td>MSP shall perform Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.</td><td></td></tr>
<tr><td>12.</td><td>Backups should be stored in such a way that disaster at either DC or DR or both should not result in loss of backups.</td><td></td></tr>
<tr><td>13.</td><td>MSP should draft an Indicative Backup plan, which will be reviewed and signed-off by MRSAC</td><td></td></tr>
<tr><td>14.</td><td>Data can only be moved to other site in case of any emergency with prior approval of MRSAC.</td><td></td></tr>
<tr><td>15.</td><td><table>
<tr><th>#</th><th>Backup Type</th><th>Backup Frequency</th><th>Retention Period</th></tr>
<tr><td>1</td><td>Incremental</td><td>Daily</td><td>7 Days</td></tr>
<tr><td>2</td><td>Full</td><td>Weekly</td><td>1 Month</td></tr>
<tr><td>3</td><td>Full</td><td>Monthly</td><td>12 Months</td></tr>
<tr><td>4</td><td>Full</td><td>Yearly</td><td>20 Years</td></tr>
</table></td><td></td></tr>
<tr><td>16.</td><td><table>
<tr><th>S No</th><th colspan="2">Restoration Policy</th></tr>
<tr><td>1</td><td>Backup taken in last month</td><td>Once in a Month</td></tr>
<tr><td>2</td><td>Backup taken in last quarter</td><td>Once in a Quarter</td></tr>
</table></td><td></td></tr>
</table>

9.5 Network Requirement

S.No.	Network Requirement General	Compliance (Yes / No)
1.	MSP must ensure that cloud virtual machine of MRSAC is into separate network tenant and virtual LAN.	
2.	MSP must ensure that cloud virtual machines are having private IP network assigned to cloud VM and should be able to communicate internally.	
3.	MSP must ensure that all the cloud VMs are in same network segment (VLAN) in single datacenter of MSP.	
4.	MSP should ensure that cloud VMs are having Internet and Service Network (internal) vNIC cards.	
5.	MSP should ensure that Internet vNIC card is having minimum 1 Gbps network connectivity and service vNIC card is on 10 Gbps for better internal communication.	
6.	In case of scalability like horizontal scalability, the MSP should ensure that additional required network is provisioned automatically of same network segment.	
7.	MSP must ensure that MRSAC gets ability to map private IP address of cloud VM to public IP address as required by MRSAC from portal of MSP.	
8.	MSP must ensure that public IP address of cloud VMs remains same even if cloud VM gets migrated to another datacenter due to any incident.	
9.	MSP must ensure that public IP address of cloud VMs remains same even if cloud VM network is being served from multiple CSP datacenters.	
10.	MSP must ensure that the public network provisioned for cloud VMs is redundant at every points.	
11.	MSP must ensure that cloud VMs are accessible from MRSAC private network used by MRSAC.	
12.	MSP should ensure that cloud VM network is IPV6 compatible.	
13.	MSP should have provision of dedicated virtual links for data replication between the datacenters in order to provide secure data replication for DR services.	
14.	MSP should ensure use of appropriate load balancers for network request distribution across multiple VMs	
15.	The Solution should allow configuring each Virtual Machine with one or more virtual NICs. Each of those network interfaces can have its own IP address and even its own MAC address.	
16.	The Solution should allow for creating virtual switches that connect virtual machines.	
17.	The Solution should support configurations of 802.1 q VLANs which are compatible with standard VLAN implementations from other vendors.	
18.	Solution should take advantage of NIC Teaming Capabilities	

S.No.	Virtual firewall	Compliance (Yes / No)
1.	Cloud infrastructure should be protected with NGFW solution with Stateful Inspection, Intrusion Prevention, Web / URL Filtering, Application Control, DoS, User Authentication, Gateway Antivirus and Sandboxing / ATP solution.	

S.No.	Virtual firewall	Compliance (Yes / No)
2.	Solution should have capability to protect against Denial of Service (DoS) attacks. Should have flexibility to configure threshold values for different anomalies.	
3.	NGFW solution should support FQDN-based address objects to resolve dynamic internal servers that can be referred in firewall policies.	
4.	The NGFW solution should have well documented and official OEM maintained default deployment templates for quick and predictable deployment.	
5.	The NGFW solution should support High Availability with such as – Single AZ / Multi-AZ HA - Native High Availability (Using API connector), Active-Active and Active-Passive with Cloud-provider Standard Load Balancer.	
6.	Cloud infrastructure should be protected from Zero Day Malware using Sandboxing technology deployed locally in the same account.	

S.No.	Server Load Balancer	Compliance (Yes / No)
1.	MSP should support Load balancing of instances across multiple host servers.	
2.	MSP should support multiple routing mechanism including round-robin. failover, sticky session etc.	
3.	MSP should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.	
4.	MSP should support an internal load balancer that routes traffic to instances within private subnets.	
5.	MSP should support health checks to monitor the health and performance of resources.	
6.	MSP should support integration with load balancer.	

S.No.	Web Application Firewall (WAF) as service	Compliance (Yes / No)
1.	Cloud platform should provide Web Application Filter for OWASP (Open web application Security project) Top 10 protection	
2.	MSP should ensure WAF should be able to support multiple website security.	
3.	MSP should ensure WAF should be able to perform packet inspection on every request covering all 7 layers.	
4.	MSP should ensure WAF should be able to block invalidated requests.	
5.	MSP should ensure WAF should be able to block attacks before it is posted to website.	
6.	MSP should ensure WAF should have manual control over IP / Subnet. i.e., Allow or Deny IP / Subnet from accessing website.	
7.	The attackers should receive custom response once they are blocked.	
8.	MSP must offer provision to customize response of vulnerable requests.	
9.	MSP should ensure WAF should be able to monitor attack incidents and simultaneously control the attacker IP.	
10.	MSP should ensure WAF should be able to Greylist or Blacklist IP / Subnet.	

S.No.	Web Application Firewall (WAF) as service	Compliance (Yes / No)
11.	MSP should ensure WAF should be able to set a limit to maximum number of simultaneous requests to the web server & should drop requests if the number of requests exceed the threshold limit.	
12.	The WAF should be able to set a limit to maximum number of simultaneous connections per IP. And should BAN the IP if the threshold is violated.	
13.	Should be able to set a limit to maximum length of path to URL.	
14.	MSP should ensure WAF to be able to limit maximum time in seconds for a client to send its HTTP request.	
15.	Should be able to BAN an IP for a customizable specified amount of time if the HTTP request is too large.	
16.	Should be able to limit maximum size of PUT request entity in MB	
17.	The WAF should be able to close all the sessions of an IP if it is banned.	
18.	Should be able to Ban IP on every sort of attack detected and the time span for ban should be customizable. There should be a custom response for Ban IP.	
19.	The Dashboard should show a graphical representation of	
	a. Top 5 Attacked Websites.	
	b. Top 5 Attacking IP.	
	c. Top 5 Attack types.	
	d. Top 5 Attacked URLs.	
20.	For analysis purpose the Dashboard should contain following information	
	a. Number of requests to web server.	
	b. Number of attacks.	
	c. Number of Attackers.	
21.	d. Types of error messages and on. of error messages sent to the users.	
22.	e. Total Bytes sent during transaction	

S.No.	Content Delivery Network (CDN) Services	Compliance (Yes / No)
1.	The service should provide ability for protection against Network and Application Layer Attacks (including DDoS attacks), Web Application Firewalls, Web Origin Protection, API Protection etc.	
2.	The service should provide ability to restrict access only to authenticated viewers.	
3.	It should be integrated with the Storage service, for easy access of documents / data using CDN	
4.	Should have sufficient point of presence in India	
5.	CDN solution implemented and commissioned for the application / system shall not degrade the performance of the original website	

9.6 Security Requirement:

S.No.	Security Requirements General	Compliance (Yes / No)
1.	MSP should ensure there is multi-tenant environment and cloud virtual resources are logically separated from others.	
2.	MSP should ensure that any OS provisioned as part of cloud virtual machine should be patched with latest security patch.	
3.	In case, the MSP provides some of the System Software as a Service for the project, MSP is responsible for securing, monitoring, and maintaining the System and any supporting software.	
4.	MSP should implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage	
5.	MSP should provide DMZ for different application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer.	
6.	MSP should give ability to create non-production environments and segregate (in a different VLAN) non-production environments from the production environment such that the users of the environments are in separate networks.	
7.	MSP should have built-in user-level controls and administrator logs for transparency and audit control.	
8.	MSP cloud platform should be protected by fully managed Intrusion detection system using signature, protocol, and anomaly-based inspection thus providing network intrusion detection monitoring	
9.	MSP should provide security services but not limited to the following: • Virtual Firewall + IPS / IDS as a Service • Virtual Web Application Firewall (WAF) • Malware Analysis – MSP shall conduct analysis of newly discovered malware to uncover its scope and origin. • DDoS service - MSP would offer DDOS Protection to protect the cloud infrastructure. Security solution shall protect against DDoS attack and provide mitigation. • The MSP shall conduct vulnerability and penetration assessment on the Cloud facility and reports shall be shared with MRSAC as per MeitY guidelines. • Security solutions to protect encryption of data in transit and at rest. MSP must provide option for use of user defined keys for encryption of data across the MRSAC cloud infrastructure	
10.	It is critical to have a set of IT security management processes and tools to ensure complete security of cloud solution. An IT security policy, framework, and operational guidelines as per ISO 27001, 27017, 27018 & PCI-DSS be maintained & implemented by Cloud service provider (MSP).	
11.	MRSAC may physically inspect the data center and will require access to the MRSAC's infrastructure as and when required by MRSAC.	
12.	All the security management processes, tools and usage shall be well documented in security policy and the security best practices to be followed to maintain IT security.	
13.	Data shall not leave the Indian boundaries and data residing within Cloud shall not be accessed by any entity outside the control of MRSAC.	
14.	MSP shall support audit features such as what request was made, possibly the source IP address from which the request was made, who made the request, when it was made, and so on.	
15.	MSP should provide read-only access for monitoring of all security tools proposed and implemented for MRSAC including but limited to Firewall, WAF, SIEM, DDOS.	

S.No.	Security Requirements General	Compliance (Yes / No)
16.	MSP should also provide on-demand full administrative access to tool / solution to MRSAC after necessary approval from MRSAC authority.	
17.	MRSAC may implement or extend any existing security solution which are used in current environment.	
18.	The CSP and MSP should meet the ever-evolving security requirements as specified by CERT-In (http://www.cert-in.org.in /).	
19.	The MSP should meet any security requirements published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the MSP by MeitY as a mandatory standard.	
20.	MSP shall be contractually subject to all GoI IT Security standards, policies, and reporting requirements. MSP shall meet and comply with all GoI IT Security Policies and all applicable GoI standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.	
21.	Information systems must be assessed whenever there is a significant change to the system's security posture.	
22.	Provide an independent Security Assessment / Risk Assessment.	
23.	All documents exclusively produced for the project are the property of the MRSAC and cannot be reproduced or retained by the MSP. All appropriate project documentation will be given to MRSAC during and at the end of this contract or at the time of termination of the contract. MSP shall not release any project information without the written consent of the MRSAC. Any request for information relating to the Project presented to the MSP must be submitted to the MRSAC for approval.	
24.	MSP shall protect all MRSAC data, etc., by treating the information as sensitive. Sensitive but unclassified information, data, will only be disclosed to authorized personnel. MSP shall keep the information confidential, use appropriate safeguards to maintain its security in accordance with minimum standards. When no longer required, this information, data, shall be returned to MRSAC control, destroyed, or held until otherwise directed by the MRSAC.	

S. No.	SIEM	Compliance (Yes / No)
1.	The solution should be scalable by adding additional receivers and still be managed through a single, unified security control panel.	
2.	The solution should be capable of real time analysis and reporting.	
3.	The platform should not require a separate RDBMS for log collection, web server or any kind of application software for its installation.	
4.	The solution should be able to assign risk scores to your most valuable asset. The risk value could be assigned to a service, application, specific servers, a user, or a group. The solution should be able to assign and consider the asset criticality score before assigning the risk score.	
5.	The activities should be separated by levels of risk for the company: very high, high, medium, low and very low.	
6.	The SIEM receiver / log collection appliance must be an appliance-based solution and not a software-based solution to store the data locally if communication with centralized correlator is unavailable.	
7.	The solution should be able to collect logs for the solutions specified in the RFP	

S. No.	SIEM	Compliance (Yes / No)
8.	The solution should provide a data aggregation technique to summarize and reduce the number of events stored in the master database.	
9.	The solution should provide a data store which is compressed via flexible aggregation logic.	
10.	The data collected from the receiver should be forwarded in an encrypted manner to SIEM log storage.	
11.	The solution should provide pre-defined report templates. The reports should also provide reports out of the box such as ISO 27002.	
12.	The solution should provide reports that should be customizable to meet the regulatory, legal, audit, standards and management requirements.	
13.	The solution should also provide Audit and Operations based report, Native support for Incident management workflow.	
14.	The solution should have single integrated facility for log investigation, incident management etc. with a search facility to search the collected raw log data for specific events or data.	
15.	A well-defined architecture along with pre and post installation document need to be shared by the bidder.	
16.	The solution should have a scalable architecture, catering multi-tier support and distributed deployment.	
17.	The solution should support collection of events / logs and network flows from distributed environment(s).	
18.	The solution should correlate security / network events to quickly prioritize its response to help ensure effective incident handling.	
19.	The solution should integrate asset information in SIEM such as categorization, criticality and business profiling and use the same attributes for correlation and incident management.	
20.	The solution should provide remediation guidance for identified security incident:	
21.	Solution should be able to specify the response procedure (by choosing from the SOPs) to be used in incident analysis / remediation.	
22.	The solution should facilitate best practices configuration to be effectively managed in a multi-vendor and heterogeneous information systems environment.	
23.	The solution should provide capability to discover similar patterns of access, communication etc. occurring from time to time, for example, slow and low attack.	
24.	The solution should share the list of out of the box supported devices / log types.	
25.	The event correlation on SIEM should be in real time and any delay in the receiving of the events by SIEM is not acceptable.	
26.	The solution should support internal communication across SIEM-components via well-defined secured channel. UDP or similar ports should not be used.	
27.	Event dropping / caching by SIEM solution is not acceptable and same should be reported and corrected immediately.	
28.	The solution should be able to facilitate customized dashboard creation, supporting dynamic display of events graphically.	

S. No.	SIEM	Compliance (Yes / No)
29.	The solution should be able to capture all the fields of the information in the raw logs.	
30.	The solution should be able to integrate logs from new devices into existing collectors without affecting the existing SIEM processes.	
31.	The solution should have capability of displaying of filtered events based on event priority, event start time, end time, attacker address, target address etc.	
32.	The solution should support configurable data retention policy based on organization requirement.	
33.	The solution should provide tiered storage strategy comprising of online data, online archival, offline archival and restoration of data.	
34.	The solution should compress the logs by at least 70% or more at the time of archiving.	
35.	The solution should have capability for log purging and retrieval of logs from offline storage.	
36.	The solution should provide proactive alerting on log collection failures so that any potential loss of events and audit data can be minimized or mitigated.	
37.	The solution should provide a mechanism (in both graphic and table format) to show which devices and applications are being monitored and determine if a continuous set of collected logs exist for those devices and applications.	
38.	The solution should support automated scheduled archiving functionality into file system.	
39.	The solution should support normalization of real time events.	
40.	The solution should provide a facility for logging events with category information to enable device independent analysis.	
41.	The platform should have High Availability Configuration of necessary SIEM components to ensure there is no single point of failure. Please describe the architecture proposed to meet this requirement.	
42.	The solution should correlate and provide statistical anomaly detection with visual drill down data mining capabilities.	
43.	The solution should have the capability to send notification messages and alerts through email, SMS, etc.	
44.	The solution should support RADIUS and LDAP / Active Directory for Authentication.	
45.	The solution should provide highest level of enterprise support directly from OEM.	
46.	Solution should support log integration for IPv4 as well as for IPv6.	
47.	Solution should provide inbuilt dashboard for monitoring the health status of all the SIEM components, data insert / retrieval time, resource utilization details etc.	
48.	Solution should support at least 100 default correlation rules for detection of network threats and attacks. The performance of the solution should not be affected with all rules enabled.	
49.	The central management console / Enterprise Security managers / receivers should be in high availability.	
50.	24 / 7 extensive monitoring of the cloud services and prompt responses to attacks and security incidents	

S. No.	SIEM	Compliance (Yes / No)
51.	Recording and analyzing data sources (e.g., system status, failed authentication attempts, etc.)	
52.	24 / 7 contactable security incident handling and troubleshooting team with the authority to act	
53.	Obligations to notify the customer about security incidents or provide information about security incidents potentially affecting the customer	
54.	Provision of relevant log data in a suitable form	
55.	Logging and monitoring of administrator activities	

S.No.	DDOS	Compliance (Yes / No)
1.	CSP should have own cloud based & DDoS scrubbing center, managed services, support public & hybrid cloud environment.	
2.	Solution should secure from system Cache poisoning, SSL / TLS encrypted, DNS reflection, DNS amplification, DNS Tunnelling, DNS Based exploits, TCP / UDP / ICMP floods, DNS protocol anomalies.	
3.	Solution should have Behavioural DoS, challenge response, CAPTCHA approach, Geolocation & IP Reputation for mitigation of flood attacks.	
4.	All layer 3, 4, and 7 DoS / DDoS threats including flood / sweep, UDP / DNS / HTTP / TCP / SIP / SYN / ACK / RST / FIN, NBA, 120+ DDoS vectors, application anomaly, dynamic filtering, protocol analysis, source tracking.	
5.	The solution should be ICSA certified & OS should be EAL or NDPP / NDcPP certified under Common Criteria Program. FIPS 140-2 Levels 3.	
6.	The solution should be an industry standard, enterprise grade	
7.	The Proposed solution should support high performance, scalable for DNS Security, DDoS, WAF, Anti-Bot features.	
8.	Should have inbuilt advance and Hardware accelerated purpose-built TLS stack for Key exchange and bulk inspection; RC4, DES, 3DES, AES-CBC, AES-GCM, AES-GMAC, RSA, ECC, DSA, DH, ECDSA, ECDH, MD5, SHA, SHA2 ciphers with FIPS 140-2 Levels	

9.7 Monitoring Requirements

S. No.	Monitoring	Compliance (Yes / No)
1.	Provide relevant tools and services for monitoring the performance, security, resource utilization etc.	
2.	Deploy agent based monitoring for Cloud infrastructure monitoring	
3.	Monitor performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications, including API access	
4.	Monitor Internet links, Replication links, MPLS, P2P (as applicable), including but not limited to Bandwidth utilization, Data transfer, Response time \(latency) and Packet loss.	
5.	Monitor Daily, weekly, monthly backup jobs as per schedule and during any unsuccessful backup the incident management process and procedures should be invoked.	

S. No.	Monitoring	Compliance (Yes / No)
6.	To perform regular health checks of VMs, Storage, N / w links, etc.	
7.	Review the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels	
8.	Implement necessary tools to monitor the root cause for performance degradation of any applications. User Department should be able to analyze whether issue is actually an Application issue or Hosting / hardware / Bandwidth issue.	
9.	Investigate outages; perform appropriate corrective action to restore the hardware, software, operating system, and related tools	
10.	Investigate outages; perform appropriate corrective action to restore the hardware, software	
11.	Any other activity associated with Monitoring Services	
12.	Provide relevant tools and services for monitoring the performance, security, resource utilization etc.	
13.	Deploy agent based monitoring for Cloud infrastructure monitoring	
14.	Monitor performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications, including API access	
15.	Monitor Internet links, Replication links, MPLS, P2P (as applicable), including but not limited to Bandwidth utilization, Data transfer, Response time \(latency) and Packet loss.	
16.	Monitor Daily, weekly, monthly backup jobs as per schedule and during any unsuccessful backup the incident management process and procedures should be invoked.	
17.	To perform regular health checks of VMs, Storage, N / w links, etc.	
18.	MSP should give provision to monitor the network traffic of cloud virtual machine.	
19.	MSP should offer provision to analyze of amount of data transferred of each cloud virtual machine.	
20.	MSP should provide network information of cloud virtual resources.	
21.	MSP should offer provision to monitor latency to cloud virtual devices from its datacenter or MRSAC should be able to set monitoring of latency to cloud VMs from outside world.	
22.	MSP must offer provision to monitor network uptime of each cloud virtual machine.	
23.	MSP must make provision of resource utilization i.e., CPU graphs of each cloud virtual machine.	
24.	MSP must make provision of resource utilization graph i.e., RAM / Storage of each cloud virtual machine. There should be provision to set alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.	
25.	MSP must make provision of resource utilization graph i.e., RAM / Storage of each cloud virtual machine.	
26.	MSP must make provision of resource utilization graph i.e., disk of each cloud virtual machine. There should be graphs of each disk partition and emails should be sent if any threshold of disk partition utilization is reached.	
27.	MSP should give provision to monitor the uptime of cloud resources. The report should be in exportable form.	

S. No.	Monitoring	Compliance (Yes / No)
28.	MSP must give provision to monitor the load of Windows, Linux etc. servers and set threshold for alerts.	
29.	MSP should make provision to monitor the running process of Windows / Linux servers. This will help MRSAC to take the snapshot of processes consuming resources.	
30.	MSP must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.	
31.	MSP must ensure that audit logs of scalability i.e., horizontal, and vertical is maintained so that billing disputes can be addressed.	
32.	MSP must ensure that log of reaching thresholds used to trigger additional resources in auto provisioning are maintained.	
33.	MSP must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity.	
34.	The MSP shall provision monitoring tools for measuring the service levels, application performance and utilization, server performance and utilization, storage performance and utilization and network performance and utilization. The tool shall be capable of providing the exact utilization of servers and shall be able to generate per day, per month and per quarter utilization reports based on which the payments will be made to the MSP.	

9.8 Usage Reporting and Billing Management

S.No.	Usage Reporting and Billing Management	Compliance (Yes / No)
1.	Track system usage and usage reports	
2.	Monitoring, managing and administering the monetary terms of SLAs and other billing related aspects.	
3.	Provide the relevant reports including real time as well as past data / information / reports for the Government	
4.	Provide relevant reports including real time as well as past data / Information / reports for MRSAC.	
5.	Summary of resolved, unresolved and escalated issues / complaints	
6.	Logs of backup and restoration undertaken report	
7.	Component wise Virtual machines availability and resource utilization report	
8.	Consolidated SLA / Non- conformance report	
9.	Any other activity associated with Reporting Services	
10.	CRUD Operations: MSP to Create, Read, Update, Delete, users based on roles & rights defined by MRSAC.	
11.	Prepare Monitoring Reports	
12.	Prepare SLA Reports	
13.	Prepare Backup Reports	
14.	Prepare VMs Status report	
15.	Provisioning / De-provisioning of VMs	
16.	Creating templates for VMs	
17.	Make changes in configurations for user administration	

S.No.	Usage Reporting and Billing Management	Compliance (Yes / No)
18.	Any other activity associated with operations and management of Cloud Management Portal	

10 Disaster Recovery Services

10.1 Overview

S.No.	Overview	Compliance (Yes / No)
1.	MSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data centre. MSP shall design and document an efficient disaster recovery solution in lines with the requirements of department and as per the RPO and RTO requirements.	
2.	The solution should be architected to run on cloud services to provide business continuity with no interruptions in case of any disruptions / disaster at DC through semi-automated processes of redirecting MRSAC data traffic to DR site.	
3.	During normal operations, the Primary Data Centre will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on hot standby. During this period, the compute environment for the application in DR shall be available as per the solution offered.	
4.	The application environment shall be installed and ready for use.	
5.	The MSP should offer switchover and switchback of individual Servers / VMs / Applications / Components instead of entire system.	
6.	Till a disaster (planned / testing or otherwise) is declared by department the users should not be allowed to access the IT applications from DR site (or as per discretion of department).	

10.2 RPO & RTO Requirements:

S.No.	RPO & RTO Requirements	Compliance (Yes / No)
1.	The service parameters to be met by the DR system focus on the Recovery Time Objective(RTO) and the Recovery Point Objective (RPO), which in business terms define the 'Interruption to Service' and 'Loss of Data' respectively. The RTO will be calculated from the time of “declaration of a disaster” up to the time by which all the applications are made fully operational & end users are able to access these applications & carry out the business operations.	
2.	The Recovery Time Objective (RTO) shall be less than or equal to 120 minutes to enable business operations & The Recovery Point Objective (RPO) should be as. - Transactional Data 15 min - Application and OS 1 Hrs.	

10.3 Replication Requirements:

S.No.	Replication Requirements	Compliance (Yes / No)
1.	MSP shall adequately do the sizing of DC-DR replication links and commission them with (1+1) redundancy, to meet the RTO and the RPO requirements.	
2.	DR Transactional Databases shall be replicated on an ongoing basis and shall be available in full (50% of the PDC) as per designed RTO / RPO and replication strategy.	
3.	The storage should be 50% of the capacity of the Primary Data Centre site.	
4.	MSP shall be responsible for providing / facilitating replication tools / software / processes for Databases, Active Directory, Web Servers, application etc. for seamless replication from DC to DR and vice versa to meet RPO and RTO requirements.	
5.	MSP shall provide detailed operating manuals for replicating these solutions.	
6.	The MSP shall deploy these tools after acquiring consent from department's project in charge.	
7.	The MSP shall provide details of replication mechanism for (but not limited to) the following solutions: - Operating system - Database - Application server - File server - Active Directory / LDAP	

DC-DR Failover & Restoration - Mock Drills / Actual Disaster:

S.No.	DC-DR Failover & Restoration - Mock Drills / Actual Disaster	Compliance (Yes / No)
1.	The MSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for complete switchover to DR.	
2.	The failover from primary DC to DR should be done through a proper DR announcement process which should be documented as part of BCP planning. In the event of a disaster, the system at proposed MSP's DR Data Center will be primary system.	
3.	The DR should be available (with its data) on-demand basis within the defined RTOs and RPOs. The users of department will connect to MSP's system through Internet link.	
4.	During the drill, the MSP shall demonstrate the fulfilment of SLAs at load of 50% users with 30% concurrency.	
5.	Application data and application states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. The installed application instance and the database shall be usable.	
6.	During the change from DC to DRC or vice-versa (regular planned changes), it should be as per the given RPO. MSP shall provide workflow-	

S.No.	DC-DR Failover & Restoration - Mock Drills / Actual Disaster	Compliance (Yes / No)
	based switchover / failover facilities (during DC failure & DR Drills). The switchback mechanism shall also be workflow based.	
7.	The Database and storage shall be of 50% capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of Data center. Users of application should be routed seamlessly from DC site to DR site.	
8.	Restoration provides an easy process for copying updated data from the DR server back to the DC server. Whenever main DC will be recovered and operational, the data from DR system to DC systems should be synchronized. Once this data is synchronized and verified, the switchover from DR system to DC system should be done. In that case all users will be accessing systems of main DC.	
9.	MSP shall provide detailed DR activity plans which will contain steps / procedures to switchover services to DR site in the event of invocation of disaster at DC site.	
10.	MSP shall also document steps for restoring services from DR site to DC site.	
11.	In case of failover to DR site (once disaster is declared) within the defined RTO, the SLA would not be applicable for RTO period only. Post the RTO period, SLA would start to apply and should be measured accordingly.	
12.	The MSP shall conduct DR drills at the interval of not more than six months of operation wherein the Primary DC must be deactivated, and complete operations shallbe carried out from the DR Site. The pre-requisite of DR drill should be carried out by MSP and department jointly. The exact process of the DR drill should be formulated in consultation with MRSAC team in a way that all elements of the system are rigorously tested, while the risk of any failure during the drill is minimized. The process should be documented by the MSP as part of the disaster recovery plan. MSP shall plan theactivities to be carried out during the mock drill and issue a notice to MRSAC at least 15 working days before such drill.	
13.	During the DR drill, the MSP need to arrange the full DR team with sufficient resources and expertise and complete the activity under the supervision of senior resource for co- ordination. The MSP shall develop appropriate policy, checklists in line framework for failover and fall back to the appropriate DR site.	

10.4 Support Third Party Audit and other requirements

S.No.	Support Third Party Audit and other requirements	Compliance (Yes / No)
1.	Provide support during Audit by STQC / MeitY empaneled agency or any agency appointed by MRSAC	
2.	Support the third party auditor / program management team / internal IT team with respect to third party audits and other requirements such as forensic investigations, SLA validation.	

10.5 Exit Management / Transition-Out Services:

S.No.	Exit Management / Transition-Out Services	Compliance (Yes / No)
1.	Continuity and performance of the Services at all times including the duration of the agreement and post expiry of the Agreement is a critical requirement of department. It is the prime responsibility of MSP during exit management period and in no way any facility / service shall be affected / degraded. Further, MSP is also responsible for all activities required to train and transfer the knowledge to department (or representative agency of department).	
2.	The exit management period starts, in case of expiry of contract, at least 3 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 MSP. The exit management period ends on the date agreed upon by department or Three months after the beginning of the exit management period, whichever is earlier.	
3.	At the end of the contract period or upon termination of contract, MSP is required to provide necessary handholding and transition support to ensure the continuity and performance of the services to the complete satisfaction of department.	
4.	Every six months, department may ask the MSP 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.	

10.6 Business Continuity Planning:

S.No.	Business Continuity Planning	Compliance (Yes / No)
1.	MSP shall define and submit (as part of the solution), a detailed approach for "Business Continuity Planning"; this should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster; further, it should define the parameters at which "disaster" would be declared.	
2.	The MSP should have a practicing framework for business continuity planning and the plan development for which has been established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.	

S.No.	Business Continuity Planning	Compliance (Yes / No)
3.	The MSP should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes.	
4.	Incident response plans should be developed by the MSP which should involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies	

10.7 Other Requirements:

S.No.	Cloud DataCenter specifications	Compliance (Yes / No)
1.	The MSP should be MeitY Empanelled and should follow all the MeitY guidelines.	
2.	The primary datacenter of the CSP should be in India at time of submission of the bid. Proposed DR site should be in a different seismic zone (within India)	
3.	All the physical servers, storage and other IT hardware from where cloud resources are provisioned for MRSAC must be within Indian datacenters only.	
4.	The MSP must be operating at least two (2) Data Centre / Disaster Recovery Centre Facilities in India at time of submission of the bid. CSP should be able to provide both DC & DR services together without any limitations as per MeitY guidelines.	
5.	The MSP datacenters should have adequate physical security in place.	
6.	The MSP datacenters should comply / certified Tier III datacenter norms.	
7.	The Data Center should conform to at least Tier III standard (preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards	

S.No.	Implementation Services	Compliance (Yes / No)
1.	Service offerings to ensure fast implementation	
2.	Services: Software install, setup.	
3.	Services: Proof of Concept setup, testing,	
4.	Services: Integration of 3rd party systems	
5.	Services: On-site Training	

S.No.	Licensing	Compliance (Yes / No)
1.	Licensing: Should be Perpetual Licensing	
2.	Licensing: No license restrictions or limitations on users	
3.	Licensing: Should not depend on no. of devices	
4.	Licensing: Availability of software updates, maintenance patches and upgrades in AMC	

S.No.	Monitoring (Near Real-time)	Compliance (Yes / No)
	Tools to ensure uptime and availability	

1.	Real-time monitoring: Ability to monitor data center devices using SNMP protocol.	
2.	Real-time monitoring: Ability to add any 3rd-party SNMP MIB and map any SNMP OID to any field	
3.	Real-time Monitoring: Ability to define thresholds	
4.	Real-time Monitoring: Alerting should be done on Mail & SMS on user defined mobile no. & mail ids.	
5.	Real-time Monitoring- Enable user-defined Croning / monitoring intervals	
6.	Real-time Monitoring- Capture threshold, events and alerts	
7.	Real-time Monitoring: Display real-time monitoring in a unified view	
8.	Real-time Monitoring: Fully Custom Dashboard	
9.	Real-time Monitoring: Capacity forecasting & circuit utilization	
10	Real-time Monitoring: Health check alerts and Device measurements	
11	Real-time Monitoring: Thermal & Energy Analytics	
12	Real-time Monitoring: ability to Monitoring Services on each device	

S.No.	Built-in reporting tools	Compliance (Yes / No)
1.	Reports: Ability to generate reports and print to PDF	
2.	Reports: Ability to export reports to 1. Excel, 2.PDF	
3.	Reports: Ability to generate graphical reports	

S.No.	Workflow / Change Management	Compliance (Yes / No)
1.	Tool should be able to manage, monitor and report on change requests	
2.	Change management: Ability to generate requests to add assets and connections.	
3.	Change management: Ability to delegate requests to other users to complete the asset / device configuration prior to submittal for review and approval.	
4.	Change management: Ability to review, reject, or approve requests.	
5.	Change management: Ability to generate e-mail notifications for every state change in the change management process.	

S.No.	User Permissions / Security	Compliance (Yes / No)
1.	Tools to ensure only the right people have the access they need.	
2.	Security: Should have 2-layer user password security for accessing device console	
3.	Permissions: Role based permissions- Site Administrator, Gatekeeper, Manager, Viewer	
4.	Permissions: Use Masters for user authentication	
5.	Access: Administrative access through web browser	
6.	Access: Can create multi-tenant in future for providing services.	
7.	Access: Support for Browsers – Internet, Mozilla and Chrome	

S.No.	Operational Management	Compliance (Yes / No)
1.	MSP should provide access of cloud virtual machines either by SSH in case of Linux and RDP in case of Windows servers.	

2.	MSP should enable MRSAC to get console access of cloud virtual machine from portal and perform operations.	
3.	MSP should upgrade its hardware from time to time to recent configuration to deliver expected performance for MRSAC.	
4.	Investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools.	
5.	MSP should manage their cloud infrastructure as per standard ITIL framework in order to delivery right services to MRSAC	

S.No.	Compatibility Requirements	Compliance (Yes / No)
1.	MSP must ensure that the virtual machine format is compatible with other cloud provider.	
2.	MSP should give provision to import cloud VM template from other cloud providers.	
3.	MSP should ensure connectivity to and from cloud resources of MRSAC to other cloud service providers if require	

S.No.	Data Management	Compliance (Yes / No)
1.	MSP should always ensure that data is destroyed whenever any cloud virtual machine is recycled or deleted. The data destruction policy of CSP should be shared with MRSAC at the time of bid submission.	
2.	MSP should clearly define policies to handle data in transit and at rest.	
3.	MSP should not delete any data at the end of agreement without consent from MRSAC.	
4.	In case of scalability like horizontal scalability, the MSP should ensure that additional generated data is modified with proper consent from MRSAC	

10.8 Project Planning and Management

The success of the project depends on the proper project planning and management. At the onset, the MSP shall plan the project implementation in great details and should provide a micro level view of the tasks and activities required to be undertaken in consultation with MRSAC. An indicative list of planning related documentation that the MSP should make at the onset is as follows:

i) **Project Schedule:** A detailed week-wise timeline indicating various activities to be performed along with completion dates and resources required for the same

ii) **Manpower Deployment List**: A list needs to be provided with resources who will be deployed on the project along with the roles and responsibilities of each resource.

iii) **Resource Deployment List**: List and number of all cloud-based resources (including but not limited to servers (VMs, storage, network components and software components) other than manpower that may be required.

iv) **Communication Plan**: Detailed communication plan indicating what form of communication will be utilized for what kinds of meeting along with recipients and frequency.

v) **Migration / Installation Plan**: The MSP will be required to submit a migration / installation plan to MRSAC for migrating the existing application on its Cloud. Necessary support will be provided by the application vendor of MRSAC.

vi) **Progress Monitoring Plan and Reporting Plan**: Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will be approved by MRSAC to the successful MSP before start of the project.

vii) **Standard Operating Procedures**: Detailed procedures for operating and monitoring the Cloud site.

viii) **Risk Mitigation Plan**: List of all possible risks and methods to mitigate them.

ix) **Escalation Matrix & Incident Management**: A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This must be via an Incident Management system.

10.9 Schedule of Events:

The MSP will have to rollout the project in three phases. The cloud resources / services that need to be commissioned during each phase are as given below along with the timelines.

S. No.	Phase	Component	Time Frame
1	Phase I	Provisioning of Cloud infrastructure for application deployment and implementation environment as per RFP	Within 20 days of issue LOA
2	Phase II	Provisioning of Cloud infrastructure for both complete DC and DR and application migration.	Within 3 months after provisioning the services as mentioned in Phase I
3	Phase III	Operation and Support	Will start from the day and date of issue of operational acceptance from MRSAC. This will be for a period of 5 years

10.10 Technical Terms and Conditions

Implementation related timelines and penalties:

i. The purpose of this Service Level Requirements / Agreement (hereinafter referred to as SLA) is to clearly define the levels of service, which shall be provided by the MSP to MRSAC for the duration of this contract period of the Project.

ii. Timelines specified in the section 9 (Work Completion Timelines and Payment Terms) shall form the Service Levels for delivery of Services specified there in.

iii. All the payments to the MSP are linked to the compliance with the SLA metrics specified in this document.

iv. The SLA are proposed to be performance based. For purposes of SLA, the definitions and terms as specified along with the following terms shall have the meanings set forth below:

v. "Uptime" shall mean the time period for which the IT Infrastructure Solution along with specified services / Components with specified technical and service standards are available for users in all in-scope Applications across the MRSAC application landscape. Uptime, in percentage, of any component (Non-IT and IT) can be calculated as Uptime = {1- [(System Downtime) / (Total Time – Planned Maintenance Time)]} * 100

vi. "Downtime" shall mean the time period for which the IT Infrastructure Solution and / or specified services / Components with specified technical and service standards are not available to users. This includes Servers, Routers, Firewall, Switches, all servers and any other IT and non-IT infrastructure, their subcomponents etc. at all Project locations etc. The planned maintenance time / scheduled downtime will include activities like software upgrades, patch management, security software installations etc.

vii. The selected MSP will be required to schedule 'planned maintenance time' with prior approval of MRSAC. This will be planned outside working time. In exceptional circumstances, MRSAC may allow the MSP to plan scheduled downtime in the working hours.

viii. "Incident" refers to any event / abnormalities in the functioning of the IT Infrastructure solution and services that may lead to disruption in normal operations.

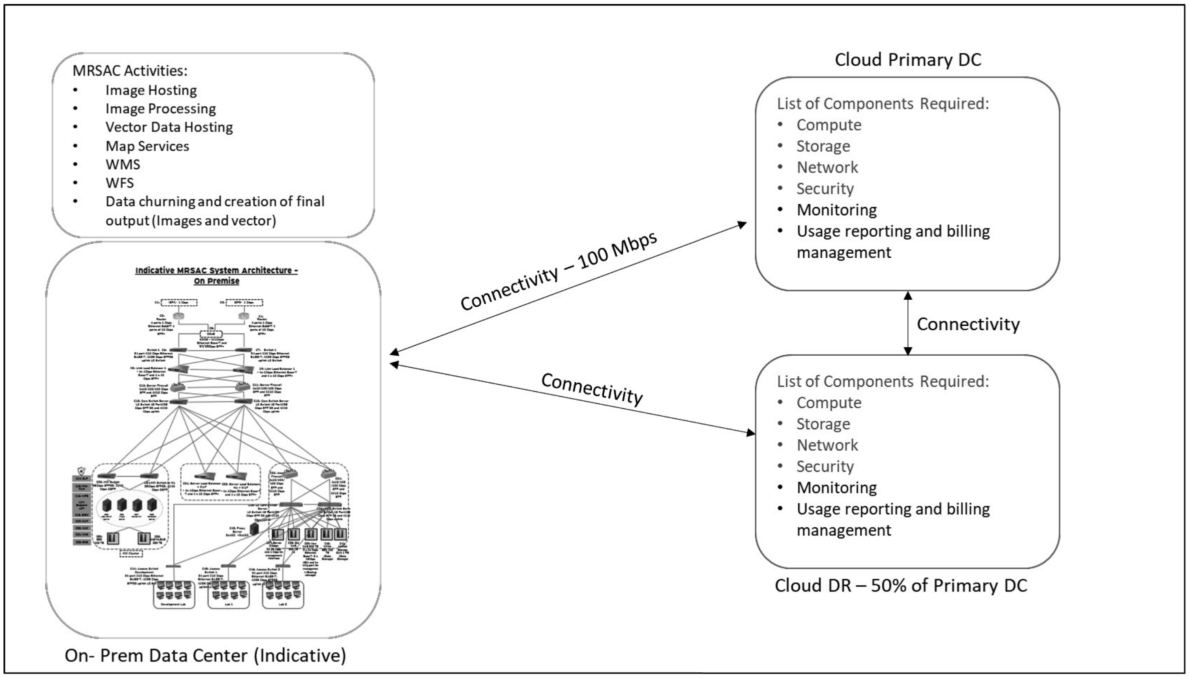
ix. "Resolution Time" shall mean the time taken (after the incident has been reported at the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level) getting the confirmatory details about the same from the MSP and conveying the same to the end user), the services related troubles during the first level escalation.

x. Commencement of SLA: The SLA shall commence from implementation period itself for adherence to the implementation plan. The penalty will be deducted from the next payment milestone during the implementation period. During the O & M period, the penalty will be deducted from the quarterly payments.

xi. MSP should provide migration, cloud deployment, managed services for primary DC and DR.

xii. The cloud services related Service Level Requirements along with their respective limits and penalties are listed in the following table

The indicative high level diagrammatic representation of the envisaged system is as below:


MRSAC Activities:
Image Hosting
Image Processing
Vector Data Hosting
Map Services
WMS
WFS
Data churning and creation of final output (Images and vector)
Indicative MRSAC System Architecture - On Premise
On- Prem Data Center (Indicative)
Connectivity – 100 Mbps
Connectivity
Cloud Primary DC
List of Components Required:
Compute
Storage
Network
Security
Monitoring
Usage reporting and billing management
Connectivity
List of Components Required:
Compute
Storage
Network
Security
Monitoring
Usage reporting and billing management
Cloud DR – 50% of Primary DC

CLOUD SERVICES REQUIREMENT OF MRSAC

11 Work Completion Timelines & Payment Terms

The payments due from MRSAC to the MSP shall comprise the following:

i. DC ProvisioningCharges: Cost of the infrastructure components provided by the vendor

ii. Disbursement of payment to the MSP is based on completion of tasks indicated in the implementation plan; Operations and Maintenance support plan and final handing over of O&M to the third party on completion at the end of five years of the contractual period.

* Payment will be based on the actual usage of the services and as per the “Unit Costs” under

Commercial Bid Format for Reference section 15.3.1

Milestone	Activity	Timeline	Payment
1	Issue of LOA	-	
2	1. Acceptance of LOA and 2. Submission of detailed implementation plan	Within 1 week of issuance of LOA	
3	1. Provisioning of Cloud resources Primary Site and 2. Setting up of the required software and OEM components 3. Testing of Cloud resources Primary Site	Within 4 weeks from the date of acceptance of LOA.	MRSAC shall begin paying 80% of the Monthly charges payable to the MSP for production DC on cloud from the date of setup of the infrastructure, OEM and software components on cloud and successful testing of the same.
4	1. Migration of applications & data on VM and other resources 2. Testing of the MRSAC production application on cloud	Within 6 weeks from the date of acceptance of LOA.	MRSAC shall begin the payment of 100% of the Monthly charges payable to the MSP for production DC on cloud from the date of successful completion of cloud migration
4	Provisioning of Cloud resources DR Site (Setting up Sync & replication between DC & DR)	Within 8 weeks from the date of acceptance of LOA.	MRSAC shall begin the payment of100% of the monthly charges towards DR on cloud from the from the date of allocation of cloud infra to the MRSAC
5	Mock Drill	Within 9 weeks from the date of acceptance of LOA.	
6	Operation and Maintenance	Will start from the date ofOperational Acceptance	Quarterly Payment after completion of each month after deduction of penalties, if any

Note:

i. If the MSP is liable for any penalty as per the SLA (refer to the related clause of this agreement), the same shall be adjusted from payments due to the MSP.

ii. Department will release the payment within 30 days of submission of valid invoice subject to the condition that invoice and all supporting documents produced are in order and work is performed as per the scope of the project and meeting the SLA Criteria. Department shall be entitled to delay or withhold the payment of a disputed invoice or part of it delivered by MSP, when department disputes such invoice or part of it, provided that such dispute is bona fide.

iii. For all items that are not covered in the current bill of material, the payment will be made based on the online rate card of the MSP.

iv. In case Go-Live is delayed, the corresponding operations and maintenance phase will start afterthe Go-Live has been completed.

v. All payments shall be made corresponding to the goods or services delivered, installed, or operationally accepted, as per the Contract Implementation Schedule, at unit prices and in the currencies specified in the Commercial Bids.

vi. Adherence to timelines is critical for the success of the project.

vii. No advance payment shall be made for any activity

viii. If the MSP is liable for any penalty as per the SLA (refer to the related clause of this agreement), the same shall be adjusted from payments due to the MSP.

ix. Quarterly bill- MRSAC will release the payment within 30 days of submission of valid invoice subject to the condition that invoice and all supporting documents produced are in order and work is performed satisfactorily as per the scope of the project duly signed by the representative of MRSAC / System In-charge and meeting the SLA Criteria. MRSAC shall be entitled to delay or withhold the payment of a disputed invoice or part of it delivered by MSP, when MRSAC disputes such invoice or part of it, provided that such dispute is bonafide.

x. No payment made by MRSAC herein shall be deemed to constitute acceptance by MRSAC of the system or any service

xi. In case Go-Live is delayed, the corresponding operations and maintenance phase will start after the Go-Live has been completed.

xii. A Project Implementation Committee (PIC) will be constituted which will be responsible for monitor the performance of the MSP and recommend for the payment.

xiii. If the MSP is liable for any penalty / liquidated damages as per the SLA, the same shall be adjusted from monthly payments due to the service provider.

xiv. All payments shall be made for the corresponding to the goods or services actually delivered, installed, or operationally accepted, per the Contract Implementation Schedule, at unit prices and in the currencies specified in the Commercial Bids.

12 Service Level Agreement (SLA) and Penalty Clause

S. No	Service Level Objective	Definition	Target	Penalty as indicated below (per occurrence)
	Delivery Schedule			
1	Meeting the Delivery schedule timeline mentioned	Provisioning and Setting up Systems and platform as per Delivery Schedule mentioned above	100 %	0.5% of the total value of the contract for delay of each Day or part thereof. The total LD shall not exceed 10% of the total value
	Service Availability			
2	Availability of following services but not limited to: 1. Virtual machines 2. Virtual Firewall 3. Load Balancer 4. DDOS Protection 5. Backup and Restore Service	Availability means, the aggregate number of hours in a calendar month during which cloud service is actually available for use through command line interface, user / admin portal and APIs (which ever applicable) Uptime Calculation for the calendar month = {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability for each of the services >= 99.95%	a) <99.95% to >= 99.00% - 10% of Monthly Payment (MP) b) <99.00% to >=
3	Availability of regular reports (SLA, Cloud Services Consumption, Monitoring, Billing and Invoicing, Security, & Project Progress)	Regular reports should be submitted within 5 working days from the end of each month.	Regular reports should be submitted within 5 working days from the end of each month.	a) <11 working days to >= 6 working days - 10% of the MP b) <16 working days to >= 11 working days - 15% of the MP c) For the delay beyond 15 days, penalty of 20% of the MP

4	Availability of the Cloud Management Portal of the CSP	Availability means the aggregate number of hours in a calendar month during which cloud management portal of the CSP is actually available for use. Uptime Calculation for the calendar month = {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability of the Cloud Management Portal of the CSP >=99.95%	a) <99.95% to >= 99.00% - 10% of the MP b) <99.00% to >= 98.50% - 15% of the MP c) <98.50% to >= 98.00% - 20% of the MP d) <98% - 30% of the MP In case the Cloud Management Portal of the CSP is not available for a continuous period of 8 Business Hours on any day, penalty shall be 50% of the MP
	Performance			
5	Provisioning of new Virtual Machine	Time to provision new Virtual Machine – Measurement shall be done by analysing the log files	95% within 15 minutes of request raised by MRSAC	a) <95% to >= 90.00% - 10% of the MP b) <90% to >= 85.0% - 15% of the MP c) <85% to >= 80.0% - 20% of the MP d) <80% - 30% of the MP
6	Spinning up the Object Storage	Time to spin up Object Storage – Measurement shall be done by analysing the log files	98% within 15 minutes of request raised by MRSAC	a) <98% to >= 95.00% - 10% of the MP b) <95% to >= 90.0% - 15% of the MP c) <90% to >= 85.0% - 20% of the MP d) <85% - 30% of the MP

7	Spinning up the Block Storage	Time to spin up to 100 GB Block Storage and attach it to the running VM – Measurement shall be done by analysing the log files	98% within 15 minutes of request raised by MRSAC	a) <98% to >= 95.00% - 10% of the MP b) <95% to >= 90.0% - 15% of the MP c) <90% to >= 85.0% - 20% of the MP d) <85% - 30% of the MP
8	Usage metric for all Cloud Services	The usage details for all the Cloud Service should be available within 15 min of actual usage – Measurement shall be done by analysing the log files and Cloud Service (API) reports	No more than 15 minutes lag between usage and Cloud Service (API reporting, for 99% of cloud services consumed	a) <99% to >= 95.00% - 10% of the MP b) <95% to >= 90.0% - 15% of the MP c) <90% to >= 85.0% - 25% of the MP d) <85% - 30% of the MP
9	Usage cost for all Cloud Service	The cost details associated with the actual usage of all the Cloud Service should be available within 24Hrs of actual usage – Measurement shall be done by analysing the log files and Cloud Service (API) reports and Invoices	No more than 24 Hrs. of lag between availability of cost details and actual usage, for 99% of cloud services consumed	a) <99% to >= 95.00% - 10% of the MP b) <95% to >= 90.0% - 15% of the MP c) <90% to >= 85.0% - 20% of the MP d) <85% - 30% of the MP
	Security			

10	Percentage of timely vulnerability reports	Percentage of timely vulnerability reports shared by CSP / MSP with within 5 working days of vulnerability identification. Measurement period is one calendar month.	Percentage of timely vulnerability reports shared within 5 working days of vulnerability identification >=99.95%	a) <99.95% to >= 99.00% - 20% of the MP b) <99.00% to >= 98.00% - 30% of the MP c) <98% - 50% of the MP
11	Percentage of timely vulnerability corrections	Percentage of timely vulnerability corrections performed by MSP. a) High Severity: Perform vulnerability correction within 7 days of vulnerability identification. b) Medium Severity: Perform vulnerability correction within 15 days of vulnerability identification. c) Low Severity: Perform vulnerability correction within 30 days of vulnerability identification. Measurement period is calendar one month.	Maintain 99.95% service Level	a) <99.95% to >= 99.00% - 20% of the MP b) <99.00% to >= 98.00% - 30% of the MP c) <98% - 50% of the MP

12	Security breach	Any incident wherein system including all cloud-based services and components are compromised or any case wherein data theft occurs (includes incidents pertaining to CSPs only)	No breach	For each breach / data theft, penalty will be levied as per following criteria: 1. Service level – Critical: Penalty of Rs 15 Lakh per incident. 2. Service level – Medium: Penalty of Rs 10 Lakh per incident. 3. Service level – Low: Penalty of Rs 5 Lakh per incident. In case of any breach of security where data is stolen, corrupted or willfully shared with other parties without the explicit consent of MRSAC, the liability clause as detailed below shall be activated and MRSAC reserves the right to terminate the contract
13	Security Incident (Malware Attack / Denial of Service Attack / Data Theft / Loss of data / Intrusion or Defacement) Applicable on the CSP's underlying infrastructure	Security incidents, as confirmed by MSP, CSP (as applicable) could consist of any of the following: Malware Attack: This shall include Malicious code infection of any of the resources, including physical and virtual infrastructure and applications. Denial of Service Attack: This shall include non-availability of any of the cloud infrastructure / service(s) due to attacks that consume related resources. The Successful MSP shall be responsible for monitoring, detecting, and resolving all Denial of Service (DoS) attacks. Intrusion: Successful unauthorized access to system, resulting in loss of confidentiality / Integrity / availability of data. The Successful MSP shall be	a) Any denial-of-service attack shall not lead to complete service non-availability. b) Zero malware attack / denial of service attack / intrusion / data theft	For each occurrence of any of the attacks (Malware attack / Denial of Service attack / Intrusion / Data Theft), 25% of the MP

		responsible for monitoring, detecting and resolving all security related intrusions on the network using an Intrusion Prevention device.		
	Support Channels - Incident Help desk			
14	Response Time	Average Time taken to acknowledge and respond once a ticket / incident is logged through one of the agreed channels. This is calculated for all tickets / incidents reported within the reporting month.	Service level – Critical: 10 Business Minutes Service level – Medium: 8 Business Hours Service level – Low: 24 Business Hours	Service level – Critical: 15% of MP for every hour of delay beyond permissible time Service level – Medium: 10% of MP for every hour of delay beyond permissible time Service level – Low: 5% of MP per hour for every hour of delay beyond permissible time
15	Resolution Time	Time taken to resolve the reported ticket / incident from the time of logging.	Service level – Critical: Within 4 hours of request Service level – Medium: Within 24 hours of request Service level – Low: Within 96 hours of request	Service level – Critical: 15% of MP for every hour of delay beyond permissible time Service level – Medium: 10% of MP for every hour of delay beyond permissible time Service level – Low: 5% of MP per hour for every hour of delay beyond permissible time
	Disaster Recovery and Backup Management			

16	Backup Recovery / Restoration Time	Measured during backup recovery / restoration.	Backup recovery / restoration time will be near zero for applications as mentioned by MRSAC during implementation	10% of the MP per every additional 2 (two) hours of downtime
17	Data loss during Backup Recovery / Restoration	Measured during backup restoration / recovery.	Data loss during backup restoration / recovery will be near zero for applications as mentioned by MRSAC during implementation	10% of the MP per every additional 2 (two) hours of data loss
18	Backup Recovery / Restoration Testing	At least two Backup Recovery / Restoration testing in a year (once every six months) or as per the agreement	At least two Backup Recovery / Restoration testing in a year (once every six months) or as per the agreement	a) No. of Backup Recovery / Restoration Testing =1 - 25% of the Yearly Payment b) No. of Backup Recovery / Restoration Testing = 0 - 50% of the Yearly Payment These will be measured every six months and the liquidated damage will be levied at the end of year Yearly payment will be considered as cumulative of monthly payments in the preceding 12 months

19	Data Migration	Migration of data from the source to destination system	Error rate <0.25%	a) Error Rate > 0.25% & <=0.30% - 15% of the MP b) Error Rate > 0.30% & <=0.35% - 20% of the MP c) Error Rate > 0.35% & <=0.40% - 30% of the MP For each additional drop of 0.05% in Error rate after 0.40%, 5% of Total MP will be levied as additional liquidity damage
	Audit and Monitoring			
20	Patch Application	Patch Application and updates to underlying infrastructure and cloud service Measurement shall be done by analysing security audit reports	95% within 8 hrs. of the notification received by MSP	a) <95% to >= 90.00% - 15% of the MP b) <90% to >= 85.0% - 20% of the MP c) <85% to >= 80.0% - 25% of the MP d) <80% - 30% of the MP
21	Budget Alerts & Notification	Alerts and Notifications for budgeting and usage-based threshold Measurement shall be done by analysing the log files and usage reports	99% within 10mins of crossing the threshold. Measurement shall be done by analysing the log files and usage reports	a) <99% to >= 95.00% - 5% of the MP b) <95% to >= 90.0% - 10% of the MP c) <90% to >= 85.0% - 15% of the MP d) <85% - 20% of the MP
22	Audit of the Sustenance of Certifications	No certification (including security related certifications mandated under MeitY empanelment such as ISO27001, ISO27017, ISO27018, ISO20001 etc.) should lapse within the Project Duration. Successful MSP should ensure the sustenance / renewal of the certificates	All certificates should be valid during the Project Duration	Delay in sustenance of certifications: a) > 1 day & <= 5 days - 10% of the MP b) > 5 day & <= 15 days - 20% of the MP c) > 15 day & <= 30 days - 30% of the MP d) > 30 days, 50% of the MP
23	Non-closure of audit observations	No observation to be repeated in the next audit	All audit observations to be closed	Penalty for percentage of audit observations repeated in the next audit a) > 0 % & <= 10% - 10% of the MP b) > 10 % & <= 20% - 20% of the MP

			within defined timelines	c) > 20 % & <= 30% - 30% of the MP d) >30% - 50% of the MP In addition, in case if MRSAC observes the lack of willingness to manage transit / sharing of information or lack of Support from MSP's end, MRSAC shall have absolute discretion to levy severe penalties and deduct the amount from monthly billing or performance bank Guarantee. During transition phase, the successful MSP shall not change or remove their key resources at any locations to enable the successful transition. In case of any such happening, MRSAC will have right to penalize the successful MSP appropriately.
24	RTO	Recovery Time Objective (RTO) which in business terms define the 'Interruption to Service'. This will be calculated Monthly	The Recovery Time Objective (RTO) shall be less than or equal to 120 minutes to enable business operations “declaration of a disaster” up to the time by which all the applications are made fully operational & end users are able to access these applications & carry out the business operations.	a) >101.50% to <= 100.75% - 10% of MP b) >100.75% to <= 101% - 15% of MP c) >101% to <= 101.5% - 20% of MP d) Subsequently, for every 0.5% increase in SLA criteria -10% of MP

25	RPO	Recovery Point Objective (RPO), which in business terms define the 'Loss of Data'. This will be calculated Monthly	The Recovery Point Objective (RPO) should be as. · Transactional Data 15 min Application and OS 1 Hrs.	a) >101.50% to <= 100.75% - 10% of MP b) >100.75% to <= 101% - 15% of MP c) >101% to <= 101.5% - 20% of MP d) Subsequently, for every 0.5% increase in SLA criteria -10% of MP

Note:

i. The MSP has to submit all the reports pertaining to SLA Review process within 7 working days after end of the quarter.

ii. All the reports must be made available to MRSAC, as and when the report is generated or as and when asked by the competent authority.

iii. In case the issue is still unresolved, the arbitration procedures described in the Terms & Conditions section 6.22 will be applicable.

iv. The down time will be calculated on monthly basis. Non-adherence to any of the services as mentioned below will lead to penalty as per the SLA clause and will be used to calculate downtime. The downtime calculated shall not include the following

a) Down time due to hardware / software and application which is owned by MRSAC at their premises

b) Negligence or other conduct of MRSAC or its agents, including a failure or malfunction resulting from applications or services provided by MRSAC or its vendors.

c) Failure or malfunction of any equipment or services not provided by the MSP.

v. However, it is the responsibility / onus of the selected MSP to prove that the outage is attributable to MRSAC. The selected MSP shall obtain the proof authenticated by the MRSAC official that the outage is attributable to the MRSAC.

vi. The total deduction per quarter shall not exceed 20% of the total QP (Quoted Price) value

vii. Two consecutive quarterly deductions amounting to more than 20% of the QPs on account of any reasons will be deemed to be an event of default and termination

viii. It is the right of the MRSAC to bring / deploy any external resources / agencies at any time for SLA review

ix. No Carry forward of any penalties of SLA calculations can be done from any of the preceding quarters

x. The Agency shall deploy sufficient manpower suitably qualified and experienced in shifts to meet the SLA. Agency shall appoint as many team members as deemed fit by them, to meet the time Schedule and SLA requirements.

xi. All SLA for the subjected bid will also be considered as per MeitY Guidelines. MSPs will also have to adhere to & accept the same accordingly

13 Technical Qualification

13.1 Technical Qualification process

The Technical Bids and related supporting documents shall be submitted online only.

i. MRSAC will review the technical bids of the short-listed MSPs to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at MRSAC discretion.

ii. The MSP's technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFP and technical evaluation framework as mentioned in Section 11.2. The MSP would be requiring covering the following but not limited to:

   a. Overall Cloud architecture including solution design

   b. Project Management and Implementation Methodology

   c. Migration Plan

   d. Integration approach with other IT Infrastructure

   e. Maintenance and Support for proposed solution

   f. Risk Mitigation plan

Final Score Calculation (QCBS):

i. The final score will be calculated through Combined Quality Based System (QCBS) method based with the following weightage:
   a. Technical: 70%
   b. Commercial :30%

Final Score	=	(0.7 X Normalised Technical Score) + (0.3 X Normalised Commercial Score)		
Normalised Technical Score of the MSP	=	Technical Score of the MSP / (divided by) Score of the MSP with highest technical score	X	100
Normalised Commercial Score of the MSP	=	Lowest Quote / (divided by) MSP Quote	X	100

- Each Technical Bid will be assigned a technical score out of a maximum of 100 marks. Only the MSPs who get an aggregate technical score of 70 marks or more will qualify for commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid and MSP.
- The work will be entrusted to the bidder having maximum final score.

13.2 Technical Evaluation Criteria

The MSP's technical proposal will be evaluated as per the requirements specified in the RFP and adopting the following evaluation criteria:

Sr. No.	Evaluation Criteria	Total Marks
1	MSP Experience – Client Citations	40
2	CV of resources	20
3	CSP partners and their capabilities	5
4	Technical Presentation	35
	Total	100

13.3 MSP's Experience

The MSP is required to provide the citations in the format placed at Annexure I Section 13.3.3 along with the supporting documents.

S. No.	Evaluation description	Criteria	Marks
1	The MSP should have experience in India of executing minimum 1 (completed / ongoing) projects of DC / DR hosting on Cloud/Private cloud/on premises with minimum value of INR 10 Crores for any State or Central Government Institution, during the last 5 years as on bid submission date.	Copy of Client certificate, work order, completion certificate or extract from the contract. • 2 Projects = 8 Marks • 1 Projects = 5 Marks • Additional 1 mark for each project of the implementation involving Hyperscale computing	10
2	The MSP / CSP must be operating at least two (2) Data Center (DC-DC, DC-DR)Facilities in India at time of submission of the bid site should be in a different seismic zone (within India)	Self-certificate from the MSP / CSP mentioning the location details signed by authorized signatory of the MSP • Two (2) DC in different seismic zone = 5 Marks • One (1) data center = 3 Marks	5
3	MSP cloud platform experience in Implementation/ Integration of GIS in any state govt. or central govt. or private data centers in India.	Experience in Implementation/ Integration of GIS in any state govt. or central govt. or private data centers in India. • Two (2) Projects with GIS - 10 Marks • One (1) Project with GIS - 5 Marks	10
4	The MSP should compulsorily possess the following certifications: • ISO 9001 • ISO 20000 • ISO 27001	Certificate of compliance • All certificate = 5 Marks	5
5	Data Centres should be compliant at a minimum with the following • Either Uptime Institute Tier III or ANSI / TIA-942-A RATING 3 certified. • ISO / IEC 27001 • ISO / IEC 27017 • ISO / IEC 27018	Copies of valid certificates. • All certificates = 5 Marks • >=3 = 3 Marks • <3 = disqualified as per Qualification sheet	5

13.4 CVs of Resources

S No	Role	Min. Qualification and Experience	Maximum Marks
1	Solution Architect	B.E. / B.Tech. / MCA 8+ years of experience in solution design	5
2	Cloud Solution Specialist	B.E. / B.Tech. / MCA 8+ years of experience in cloud solution implementation, monitoring and management	5
3	DevOps and Microservices Consultant	B.E. / B.Tech. / MCA 5+ years of experience in implementation and management of DevOps environment using microservices	5
4	Open-Source Stack consultant	B.E. / B.Tech. / MCA 8+ years of experience in Open-source software installation, configuration, and management on cloud	5

13.5 Capabilities in service provisioning across CSPs

S. No.	Evaluation Description	Criteria	Marks
1	Experience in providing Cloud solution and managed services for DC / DR across multiple CSP's	3 Projects= 10 Marks 2 Projects = 8 Marks 1 Project = 6 Mark	10

13.6 Technical Presentation

Role	Evaluation Criteria	Maximum Marks
Technical Presentation	• MSP's understanding level of the scope of work (5 Marks) • Proposed Solution on cloud (10 Marks) • Project Management Methodology for Development Phase (5 Marks) • Project Management Methodology for Implementation Phase (5 Marks) • Project Management Methodology for the O &M Phase (5 Marks) • MSPs' awareness of the risks in the project (5 Marks)	35

14 Draft Contract Agreement

14.1 Definitions, Interpretations and Other Terms

i. Bid means the tender process conducted by MRSAC and the technical and commercial proposals submitted by the successful MSP, along with the subsequent clarifications and undertakings, if any.

ii. 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);

iii. Customers mean all citizens and business organization and users who use the MRSAC services.

iv. Deliverables means all the activities related to the Cloud and other service provisioning, as defined in the Bid Document & subsequent Corrigendum (if any), based on which the technical proposal & commercial proposal was submitted by the MSP and as required as per this CA.

v. Effective Date means the date on which the Purchase Order or Letter of Acceptance is issued.

vi. CA means this Contract Agreement, together with the recitals and all schedules and the contents, requirements, specifications, and standards of the Bid Document (as may be 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.

vii. Performance Security means the irrevocable and unconditional Bank Guarantee provided by the Service provider from any Nationalized / Scheduled bank in favor of <<Official Name>>, an amount of INR 50 Lakhs.

viii. 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 / after the execution of this contract.

ix. Required Consents means the written consents, clearances and licenses, rights and other authorizations as may be required to be obtained by the Service Provider, for all tasks / activities / software / hardware and communication technology for this project; from all the concerned departments / agencies, etc. as the case may be.

x. Bid Document means the Request for Proposal released and includes all clarifications / addendums, explanations and amendments issued by MRSAC in respect thereof.

xi. Services means the content and services delivered and to be delivered to the customers or the offices of MRSAC by the Service Provide

xii. Users means MRSAC staffs or any other MRSAC officials having access to MRSAC Application Landscape including its Implementation Agencies, technology vendors, corporations and agencies and their employees, as the context admits or requires.

14.2 Interpretations

i. 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.

ii. Words denoting the singular shall include the plural and vice-versa and words denoting persons shall include firms and corporations and vice versa.

iii. Unless otherwise expressly stated, the words “herein”, “hereof”, “hereunder” and similar words refer to this CA as a whole and not to any 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 hard copy, unless otherwise stated.

iv. 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.

v. 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.

vi. 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.

vii. References to "construction" or "roll out" includes, unless the context otherwise requires, design, development, implementation, engineering, procurement, delivery, transportation, installation, processing, fabrication, acceptance testing, certification, commissioning, and other activities incidental to the construction or roll out, and "construct" or "roll out" shall be construed accordingly.

viii. Any word or expression used in this CA shall, unless defined or construed in this CA, bear its ordinary English language meaning.

ix. 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.

x. 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 Service Provider.

xi. MRSAC 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

xii. The agency / individual nominated by MRSAC can engage professional organizations for conducting specific tests on the software, hardware, networking, security, and all other aspects.

xiii. The agency / individual will establish appropriate processes for notifying the Service Provider of any deviations from the norms, standards, or guidelines at the earliest instance after taking cognizance of the same to enable the Service Provider to take corrective action.

xiv. Such an involvement of and guidance by the agency / person will not, however, absolve the Service Provider of the fundamental responsibility of designing, installing, testing, and commissioning the application & the infrastructure for efficient and effective delivery of services as contemplated under this Bid Document.

xv. 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:

a. Scope of Services for the MSP

b. Detail Commercial proposal of the MSP accepted by MRSAC

c. Clarification & Corrigendum Documents published by MRSAC after the Bid

Document for this work

a. Bid Document of MRSAC for this work

b. RFP issued by MRSAC to the successful MSP and

c. Successful MSP "Technical Proposal" and "Commercial Proposal" submitted in response to the Bid Document.

14.3 Term of the Contract Agreement

i. The term of this CA shall be a period of Five years from the date of issuance of Letter of Acceptance / Purchase Order. This includes the time required for managed cloud service provisioning, including co-location.

ii. In the event of implementation period getting extended beyond the stipulated time, for reasons not attributable to the MSP, MRSAC reserves the right to extend the term of the Agreement by corresponding period to allow validity of contract from the date of operational acceptance.

14.4 Professional Project Management:

MSP shall execute the project with complete professionalism and full commitment to the scope of work and the prescribed service levels. MSP shall attend regular Project Review Meetings scheduled by MRSAC and shall adhere to the directions given during the meeting. Following responsibilities are to be executed by the MSP 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, IT Infrastructure Management Plan, etc.

b) Preparation and regular update of the Risk Register and the Mitigation Plan. Timely communication of the same to all the identified project stakeholders

c) Submission of Weekly Project Progress Reports

d) Monthly Compliance report, which will cover compliances to Project Timelines, Hardware and Software delivered, SLAs, etc.

14.5 Use & Acquisition of Assets during the term

The MSP shall:

i. Take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components used for the project and other facilities leased / owned by the MSP exclusively in terms of the delivery of the services as per this CA (hereinafter the “Assets”) in proportion to their use and control of such Assets which will include all upgrades / enhancements and improvements to meet the needs of the project arising from time to time

ii. Term “Assets” also refers to all the hardware / Software / furniture / data / documentations / manuals / or any other material procured, created or utilized by the MSP or MRSAC for implementation of IT Infrastructure solution.

iii. Keep all the tangible Assets in good and serviceable condition (reasonable wear and tear excepted) suitably upgraded subject to the relevant standards as stated in the bid to meet the SLAs mentioned in the contract and during the entire term of the Agreement

iv. Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of Assets, and which are provided to the MSP will be followed by the MSP and any person who will be responsible for the use of the Asset

v. Take such steps as may be recommended by the manufacturer of the Assets and notified to the MSP or as may be necessary to use the Assets in a safe manner

vi. To the extent that the Assets are under the control of the MSP, keep the Assets suitably housed and in conformity with any statutory requirements from time to time applicable to them

vii. 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

viii. Use the Assets exclusively for the purpose of providing the Services as defined in the contract

ix. Ensure the integration of the software with hardware to be setup and the current Assets in order to ensure the smooth operations of the entire solution architecture to provide efficient services to MRSAC of this Project in an efficient and speedy manner

14.6 Security and Safety

i. The MSP will 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

ii. Adherence to basic e-Governance Guidelines and Standards for data structure (if any) shall be adhered to.

iii. MSP shall also comply with MRSAC information technology security and standard policies in force from time to time as applicable. MRSAC shall share the relevant guidelines and standards to the MSP upon signing of the CA.

iv. MSP shall use reasonable endeavours to report forthwith in writing to all the partners / contractors about the civil and criminal liabilities accruing due to any unauthorized access (including unauthorized persons who are employees of any Party) or interference with MRSAC data, facilities or Confidential Information.

v. The MSP shall upon reasonable request by MRSAC or his / her nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.

vi. MSP 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 at MRSAC.

14.7 Performance Bank Guarantee

i. The MSP shall at its own expense, deposit with department, within 30 days of the notification of award (done through issuance of the Purchase Order / Letter of Acceptance), an unconditional and irrevocable Performance Bank Guarantee (PBG) from nationalized / Scheduled Bank as per the format placed at Section 15.1 of this Bid Document, payable on demand, for the due performance and fulfilment of the contract by the MSP. This Performance Bank Guarantee will be for an amount of INR 50 Lakhs or 10% of the value of the order valid for five years. All charges whatsoever such as premium, commission, etc. with respect to the PBG shall be borne by the MSP.

ii. The PBG would be valid for a period of 3 more months from the date of validity of the Contract. The PBG may be discharged / returned by department upon being satisfied that there has been due performance of the obligations of the MSP under the contract. However, no interest shall be payable on the PBG. In the event, MSP being unable to service the contract for whatever reason, department would evoke the PBG. Notwithstanding 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 MSP's failure to complete its obligations under the Contract. Department shall notify the MSP in writing of the exercise of its right to receive such compensation within 14 days, indicating the contractual obligation(s) for which the MSP is in default.

iii. Department shall also be entitled to make recoveries from the MSP's bills, PBG, or from any other amount due to him, the equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction, or misstatement.

14.8 Indemnity

i. The MSP agrees to indemnify and hold harmless MRSAC, its officers, employees and agents(each an “Indemnified Party”) promptly upon demand at any time and from time to time, from and against any and all losses , claims, damages, liabilities, costs (including reasonable attorney’s fees and disbursements) and expenses (collectively, “Losses”) to which the Indemnified Party may become subject, in so far as such losses directly arise out of, in any way relate to, or result from any misstatement or any breach of any representation or warranty made by the MSP

Or

ii. The failure by the MSP 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 MSP. Against all losses or damages arising from claims by third Parties that any Deliverable (or the access, use or other rights thereto), created by MSP pursuant to this Agreement, or any equipment, software, information, methods of operation or other intellectual property created by MSP pursuant to this Agreement, or the SLAs (I) infringes a copyright, trade mark, trade design enforceable in India, (II)infringes a patent issued in India, or (III) constitutes misappropriation or unlawful disclosure or use of another Party’s trade secretes under the laws of India (collectively,

iii. “Infringement Claims”); provided, however, that this will not apply to any Deliverable (or the access, use or other rights thereto) created by “Implementation of the IT Infrastructure product by itself at the direction of MRSAC, or

iv. Any compensation / claim or proceeding by any third party against MRSAC arising out of any act, deed, or omission by the MSP or

v. Claim filed by a workman or employee engaged by the MSP 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. Any payment made under this Agreement to an indemnity or claim for breach of any provision of this Agreement shall include applicable taxes.

14.9 Third Party Claims

i. Subject to Sub-clause (b) below, the MSP (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 or 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.

ii. The indemnities set out in Sub-clause (a) above shall be subject to the following conditions:

iii. 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.

iv. 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.

v. 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 it may deem appropriate, and the cost and expense of the Indemnified Party will be borne and paid by the Indemnifying Party.

vi. 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.

vii. MSP hereby indemnify and hold indemnified MRSAC harmless from and against all damages, losses, liabilities, expenses including legal fees and 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.

viii. 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 and include an unconditional release to the Indemnified Party from the claimant for all liability in respect of such claim; and (b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement.

ix. 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; and

x. 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 and defenses of the Indemnified Party with respect to the claims to which such indemnification relates.

xi. 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 (PBG), if such indemnity is not paid, either in full or in part, and on the invocation of the Performance Bank Guarantee, the Indemnifying Party shall be subrogated to all rights and defenses of the Indemnified Party with respect to the claims to which such indemnification relates. The format for PBG is placed at Section 15.1.

xii. MSP will defend or settle third party claims against MRSAC solely attributable to the MSP's infringement of any copyrights, trademarks or industrial design rights alleged to have occurred in respect of MSP branded hardware / software / deliverables etc. (together "deliverables") supplied by the MSP. The MSP shall pay all costs, damages and attorney's fees that a court finally awards.

xiii. MRSAC shall provide the MSP with prompt notice of such claim and extend full cooperation and assistance, information and authority reasonably necessary to defend or settle such claim. The MSP will have adequate opportunity to control the response thereto and the defense thereof.

xiv. Further as an exclusion, the MSP shall have no obligation for any claim of infringement to the extent arising from use of the deliverables in a way not indicated in the statement of work or in any specifications or documentation provided with such deliverable

14.10 Warranties

The MSP 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 MSP.

iii. It shall discharge its obligations under this Agreement with due skill, care, and diligence to comply with the service level agreement.

iv. In the case of the SLAs, the MSP warrants and represents to MRSAC, that:

v. The MSP has full capacity and authority and all necessary approvals to enter and perform its obligations under the SLAs and to provide the Services.

vi. The SLAs shall be executed by a duly authorized representative of the MSP.

vii. The Services will be provided and rendered by appropriately qualified, trained, and experienced personnel as mentioned in the bid.

viii. MSP 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.

ix. The Services will be supplied in conformance with all laws, enactments, orders, and regulations applicable from time to time.

x. MSP will warrant that the solution provided under the contract is new, of the most recent higher version / models and incorporate all recent improvements in design and materials unless provided otherwise in the contract.

xi. The MSP shall ensure defect free operation of the entire solution and shall replace any such components, equipment, software and hardware which are found defective and during the entire contract period the MSP shall apply all the latest upgrades / patches / releases for the software after appropriate testing. No costs shall be paid separately for warranty other than what are the cost quoted by the MSP and as specified in the contract.

xii. If the MSP 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.

xiii. Notwithstanding what has been stated elsewhere in this Agreement and the Schedules attached herein, in the event the MSP is unable to meet the obligations pursuant to the Implementation of the IT Infrastructure Solution, Operations and Maintenance Services and any related scope of work as stated in this Agreement and the Schedules attached herein, MRSAC will have the option to invoke the Performance Guarantee after serving a written notice of thirty (30) days to the MSP

xiv. The 30-day notice period shall be considered as the 'Cure Period' to facilitate the MSP to cure the breach. The PBG of entire amount shall be evoked only if the breach is solely attributable to the MSP and the MSP fails to rectify the breach within the 'Cure Period'.

14.11 Force Majeure

The MSP shall not be liable for forfeiture of its Performance Guarantee, imposition of liquidated damages or termination for default, if and to the extent that it's delay 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 MSP, not involving the MSP's fault or negligence and not foreseeable. Unforeseen circumstances or causes beyond the control of the MSP include but are not limited to acts of God, war, riot, acts of civil or military authorities, fire, floods, accidents, terrorist activity, strikes or shortages of transportation facilities, fuel, energy, labor or material.

For the MSP to take benefit of this clause it is a condition precedent that the MSP must promptly notify MRSAC, in writing of such conditions and the cause thereof within five calendar days of the arising of the Force Majeure event. MRSAC, or the consultant / committee appointed by MRSAC shall study the submission of the MSP and inform whether the situation can be qualified one of Force Majeure. Unless otherwise directed by MRSAC in writing, the MSP 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 MSP 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 MSP.

14.12 Resolution of Disputes

MRSAC and the MSP shall make every attempt to resolve dispute amicably, by direct information, negotiations of any disagreement or dispute arising between them under or in connection with this agreement. All differences disputes arising under and out of these present, or in connection with this agreement shall be first referred to the senior executives of each party for an amicable solution. If the dispute is not resolved within a period of thirty (30) days, the same shall be referred to arbitration in accordance with Arbitration and Conciliation Act, 1996 (including all amendments thereto). Each party shall appoint one arbitrator each and the two appointed arbitrators shall appoint the third arbitrator. The decision of the arbitrators shall be final and binding on both parties. The venue of arbitration shall be Maharashtra, India. Subject to the above, this Agreement shall be subject to the jurisdiction of the courts in Maharashtra, India.

14.13 Limitation of Liability towards MRSAC

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

MSP's aggregate liability in connection with obligations undertaken as a part of this contract regardless of the form or nature of the action giving rise to such liability, shall be at actual and limited to the amount paid by MRSAC for:

i. the particular hardware / software; or
ii. services provided during the twelve (12) months immediately preceding the date of the claim; that in each case is the subject of the claim.

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

14.14 Conflict of Interest

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

ii. In the event of any question, dispute or difference arising under the agreement or in connection there-with, the same shall be referred to the sole arbitration of the Director, MRSAC or in case his designation is changed or his office is abolished, then in such cases to the sole arbitration of the officer for the time being entrusted (whether in addition to his own duties or otherwise) with the functions of the Director, MRSAC or by whatever designation such an officer may be called (hereinafter referred to as the said officer), and if the Chairman of Board or the said officer is unable or unwilling to act as such, then to the sole arbitration of some other person appointed by the Chairman of Board or the said officer.

iii. The agreement to appoint an arbitrator will be in accordance with the Arbitration and Conciliation Act 1996. There will be no objection to any such appointment on the ground that the arbitrator is a Government Servant or that he has to deal with the matter to which the agreement releasor that in the course of his duties as a Government Servant he has expressed his views on Allor any of the matters in dispute.

iv. The award of the arbitrator shall be final and binding on both the parties to the agreement. In the event of such an arbitrator to whom the matter is originally referred, being transferred or vacating his office or being unable to act for any reason whatsoever, the Chairman of Board, MRSAC or the said officer shall appoint another person to act as an arbitrator in accordance with terms of the agreement and the person so appointed shall be entitled to proceed from the stage at which it was left out by his predecessors.

v. The arbitrator may from time to time with the consent of both the parties enlarge the time

vi. frame for making and publishing the award. Subject to the aforesaid, arbitration and Conciliation Act, 1996 and the rules made there under, any modification thereof for the time being in force shall be deemed to apply to the arbitration proceeding under this clause.

vii. The venue of the arbitration proceeding shall be the office of the Chairman of Board, MRSAC, or such other places as the arbitrator may decide.

14.15 Data Ownership

All the data created as the part of the project shall be owned by MRSAC. The MSP shall take utmost care in maintaining security, confidentiality and backup of this data. MRSAC shall retain ownership of any user created / loaded data and applications hosted on MSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.

14.16 Fraud and Corruption

i. MRSAC requires that MSP 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:

ii. "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of MRSAC in contract executions.

iii. "Fraudulent practice" means a misrepresentation of facts, in order to influence a procurement process or the execution of a contract, to MRSAC, and includes collusive practice among MSPs (prior to or after bid submission) designed to establish bid prices at artificially high or non-competitive levels and to deprive MRSAC of the benefits of free and open competition

iv. "Undesirable practice" means (i) establishing contact with any person connected with or employed or engaged by MRSAC with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest;

v. "Restrictive practice" means forming a cartel or arriving at any understanding or arrangement among MSPs with the objective of restricting or manipulating a full and fair competition in the Selection Process.

vi. "Coercive Practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract.

vii. If it is noticed that the MSP has indulged into the Corrupt / Fraudulent / Undesirable / Coercive practices (as be decided by a court or competent authority with appropriate jurisdiction), it will be a sufficient ground for MRSAC for termination of the contract and initiate blacklisting of the vendor.

14.17 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 3 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 MSP. The exit management period ends on the date agreed upon by MRSAC or Three months after the beginning of the exit management period.

ii. Confidential Information, Security and Data

MSP will promptly, on the commencement of the exit management period, supply to MRSAC or its nominated agencies the following:

a. Project data as is reasonably required for purposes of the project or for transitioning of the services to its replacing successful MSP in a readily available format.

b. 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 may be).

c. The MSP shall retain all of the above information with them for 45 days after the termination of the contract, post which the provider has to wipe / purge / delete all information created or retained as part of this project.

d. MSP will sign a Non-Disclosure Agreement with MRSAC.

e. MSP shall ensure deploying software and software tools for the cloud solution maintaining industry standards.

f. The MSP shall ensure availability of required infrastructure to manage the implemented cloud solution with the in-coming vendor post exit. Plan for this shall be made by the MSP and presented to MRSAC and in due consultation with other stakeholders of the project.

iii. Employees

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

iv. Other conditions

a. The MSP shall not delete any data at the end of the agreement from the underlying MSP's Cloud environment (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Purchaser. The Purchaser shall pay to the MSP the cost associated with retaining the data beyond 45 days. The associated cost shall be arrived at based on the cost figures indicated in the commercial quote submitted by the MSP.

b. The underlying MSP shall be responsible for providing the tools for import / export of VMs, associated content, data, etc., and the MSP, in consultation with the Purchaser, shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition related activities.

c. The MSP shall provide the Purchaser or its nominated agency with a recommended exit management plan ("Exit Management Plan") or transition plan indicating the nature and scope of the underlying MSP's transitioning services. The Exit Management Plan shall deal with the following aspects of the exit management in relation to the Agreement as a whole or the particular service of the Agreement:

- Transition of Managed Services
- Migration from the incumbent MSP Cloud Service Provider's environment to the new environment

d. The MSP is responsible for both transition of the services as well as migration of the VMs, Data, Content and other assets to the new environment.

e. The Managed Service Provider shall carry out the migration of the VMs, data, content and any other assets to the new environment (alternate Cloud Service Provider or Data Centre) identified by the Purchaser to enable successful deployment and running of the Purchaser's solution in the new environment.

f. The format of the data transmitted from the current CSP to the new environment identified by MRSAC should leverage standard data formats (e.g., OVF, etc.) whenever possible to ease and enhance portability. The format shall be finalized in consultation with the Purchaser.

g. The MSP shall transition Purchaser's solution including retrieval of all data in the formats approved by the Purchaser.

h. The MSP shall ensure that all the documentation required by the Purchaser for smooth transition (in addition to the documentation provided by the underlying Cloud Service Provider) are kept up to date and all such documentation is handed over to the Purchaser during regular intervals as well as during the exit management process.

i. The MSP shall transfer the organizational structure developed during the term to support the delivery of the Exit Management Services.

This will include:

i. Documented and updated functional organization charts, operating level agreements with third-party contractors, phone trees, contact lists, and standard operating procedures.

ii. Physical and logical security processes and tools, including catalogues, badges, keys, documented ownership and access levels for all passwords, and instructions for use and operation of security controls.

iii. The MSP shall carry out following key activities, including but not limited to, as

part of the knowledge transfer:

a. Preparing documents to explain design and characteristics

b. Carrying out joint operations of key activities or services

c. Briefing sessions on processes and documenting processes

d. Sharing the logs, etc. e. Briefing sessions on the managed services, the way these are deployed on Cloud and integrated

e. Briefing sessions on the offerings (IaaS / PaaS / SaaS) of the underlying Cloud Service Provider

f. The Managed Service Provider shall transfer know-how relating to operation and maintenance of the solution, software, Cloud Services, etc.

iv. Exit Management Plan

Successful MSP 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.

a. 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.

b. Plans for the communication with such of the Successful MSP, 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.

c. Plans for provision of contingent support to the implementation of IT Infrastructure Solution for a reasonable period (minimum one month) after transfer.

d. Exit Management Plan shall be presented by the MSP to and approved by MRSAC or its nominated agencies.

e. The terms of payment as stated in the Terms of Payment Schedule include the costs of the

MSP complying with its obligations under this Schedule.

a. During the exit management period, the MSP shall use its best efforts to deliver the services.

b. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

c. Rights of Access to Information

At any time during the exit management period, the MSP 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, catalogues, archive data, Live data, policy documents or any other material related to implementation of IT Infrastructure Solution for MRSAC.

14.18 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 MSP and terminate the contract either in whole or in part:

i. Where MRSAC is of the opinion that there has been such Event of Default on the part of the

ii. service provider which would make it proper and necessary to terminate this Contract and

iii. may include failure on the part of the service provider to respect any of its commitments with regard to any part of its obligations under its bid, the RFP or under this Contract

iv. Where it comes to MRSAC attention that the service provider is in a position of actual conflict of interest with the interests of MRSAC, in relation to any of services arising out of

v. services provided under the resultant contract or this RFP

vi. If the MSP fails to deliver any or all of the project requirements / operationalization / Operational Acceptance of project within the time frame specified in the contract; or

vii. If the MSP fails to perform any other obligation(s) under the contract.

viii. Prior to providing a notice of termination to the MSP, MRSAC shall provide the MSP with a written notice of 30 days instructing the MSP to cure any breach / default of the Contract, if MRSAC is of the view that the breach may be rectified.

ix. On failure of the MSP to rectify such breach within 30 days, MRSAC may terminate the contract by providing a written notice of 30 days to the MSP, 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 an event the MSP shall be liable for penalty imposed by MRSAC.

x. 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

xi. ensure an efficient transition and effective continuity of the services which the MSP 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 MSP in relation to the execution / continued execution of the requirements of this contract.

14.19 Confidentiality

i. Service provider shall maintain the highest level of secrecy, confidentiality and privacy with regard thereto.

ii. Additionally, the service provider shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems / facilities.

iii. MRSAC shall retain all rights to prevent, stop and if required take the necessary punitive action against the service provider regarding any forbidden disclosure.

iv. Service provider should provide non-disclosure agreement, which shall be duly approved by the MRSAC

For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

a) Information already available in the public domain.
b) Information which has been developed independently by the service provider
c) Information which has been received from a third party who had the right to disclose the aforesaid information.
d) Information which has been disclosed to the public pursuant to a court order.

14.20 Miscellaneous

i. 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 (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 MSP (including all partners) 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 MSP and its Personnel make public the recommendations formulated in the course of, or as a result of the project. In matters pertaining to privacy of data, the MSP (including all partners) shall not use any data for analytical / commercial reasons whatsoever.

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

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; and
ii. Was in the recipient's possession free of any obligation of confidence prior to the time of receipt of it by the Recipient hereunder; and
iii. Is developed by the Recipient independently of any of discloser's Confidential Information; and
iv. Is rightfully obtained by the Recipient from third Parties authorized at that time to
v. make such disclosure without restriction; and
vi. Is identified in writing by the Discloser as no longer proprietary or confidential; or
vii. Is required to be disclosed by law, regulation, or Court Order, provided that the recipient
viii. gives prompt written notice to the Discloser of such legal and regulatory requirement
ix. to disclose so as to allow the Discloser reasonable opportunity to contest such disclosure.
x. To the extent that such disclosure is required for the purposes of this Agreement, either Party may disclose Confidential Information to:

   a. Its employees, agents and independent contractors and to any of its affiliates and their respective independent contractors or employees; and
   b. Its professional advisors and auditors, who require access for the purposes of this Agreement, whom the relevant Party has informed of its obligations under this Article and 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.

The provisions of this Article shall survive the expiration or any earlier termination of this Agreement.

ii. Standards of Performance

The MSP 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 MSP shall always act in respect of any matter relating to this contract. The MSP shall abide by all the applicable provisions / Acts / Rules Regulations, Standing orders, etc. of Information Technology standard as prevalent in the country. The MSP shall also conform to the standards laid down by or Government of India from time to time. Such standards and guidelines shall be shared with the MSP by MRSAC up on signing of the Contract.

a. Subcontracts: There should be no sub-contracting for the cloud services of MSP activities.

b. Care to be taken while working at MRSAC Office

MSP should follow instructions issued by concerned Competent Authority from time to time for carrying out work at designated places. MSP should ensure that there is no damage caused to any private or public property. In case such damage is caused, MSP shall immediately bring it to the notice of concerned organization and MRSAC in writing and pay necessary charges towards fixing of the damage.

MSP shall ensure that its employees / representatives don’t breach privacy of any citizen or establishment during the course of execution or maintenance of the project.

iii. Compliance with Labor regulations

The MSP 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 MRSAC project should be paid using ECS / NEFT / RTGS. A record of the payments made in this regard should be maintained by the MSP. Upon request, this record shall be produced to the appropriate authority in MRSAC and / or Judicial Body. If complaints are received by MRSAC (or any appropriate authority) appropriate action (Liquidation of Security Deposit, Blacklisting, etc.) may be initiated as deemed necessary against the MSP.

iv. 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.

v. 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.

vi. 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,

MSP:

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 9.30 am and 5.30 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).

vii. Personnel / Employees

Personnel / employees assigned by MSP to perform the services shall be employees of MSP, and under no circumstances will such personnel be considered as employees of MRSAC. MSP shall have the sole responsibility for supervision and control of its personnel and for payment of such personnel's employee's entire compensation, including salary, legal deductions withholding of income taxes and social security taxes, worker's compensation, employee and disability benefits and the like and 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 MSP.

MSP shall use its best efforts to ensure that sufficient MSP personnel are employed to perform the Services, and 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 MSP personnel performing work under this Agreement. In the event that MRSAC requests that any MSP personnel be replaced, the substitution of such personnel shall be accomplished pursuant to a mutually agreed upon schedule and upon clearance of the personnel based on profile review and personal interview by MRSAC or its nominated agencies as per defined SLAs. The MSP shall depute quality team for the project and as per requirements MRSAC shall have the right to ask MSP to change the team.

a. Management (Regional Head / VP level officer) of MSP needs to be involved in the project monitoring and should attend the review meeting at least once in a month.
b. The profiles of resources proposed by MSP in the technical bid, which are considered for technical bid evaluation, shall be construed as 'Key Personnel' and the MSP shall not remove such personnel without the prior written consent of MRSAC. For any changes to the proposed resources, MSP shall provide equivalent or more experienced resources in consultation with MRSAC.
c. Except as stated in this clause, nothing in this Agreement will limit the ability of MSP freely to assign or reassign its employees; provided that MSP 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 and approve MSP's plan for any such knowledge transfer. MSP shall maintain the same standards for skills and professionalism among replacement personnel as in personnel being replaced.
d. Each Party shall be responsible for the performance of all its obligations under this Agreement and shall be liable for the acts and omissions of its employees and agents in connection therewith.

viii. Variations & Further Assurance

a. 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.

b. 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.

ix. Severability & Waiver

a. 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 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.

b. 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.

x. 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 of by implication intended to come into effect or continue in effect after such expiry or termination.

14.21 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 New Delhi courts only.

Attachments to the Agreement:

i) Scope of Services for the MSP

ii) Detail Commercial proposal of the MSP accepted by MRSAC

iii) Corrigendum Document published by MRSAC subsequent to the Bid Document for this work

iv) Bid Document of MRSAC for this work

v) LoI issued by MRSAC to the successful MSP

vi) The successful MSP's "Technical Proposal" and "Commercial Proposal" submitted in response to the Bid Document

15 Annexure I:

15.1 Instructions for Pre-Qualification Bid

15.1.1 Pre-Qualification Cover Letter

Date: dd / mm / yyyy

To

MRSAC Name and Address

Sub: Request for Proposal for Selection of Managed Service Provider MSP for procurement of Cloud services to MRSAC under MahaBHUMI Project of Govt. of Maharashtra for DC and DR for 5 years

Ref: Tender No: <No> Dated <DD / MM / YYYY>

Dear Sir,

We, the undersigned, offer to provide MSP services to MRSAC with reference to your Request for Proposal dated **<insert date>** and our Proposal. We are hereby submitting our Pre- qualification bid.

We hereby declare that all the information and statements made in this Pre- qualification bid are true and accept that any misinterpretation contained in it may lead to our disqualification.

We agree to abide by all the terms and conditions of all the volumes of this RFP document. We would hold the terms of our proposal valid for 180 number of days from the date of submission of the proposal.

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.

____

Signature of Authorized Signatory (with official seal) Name :

Designation :

Address :

Telephone & Fax :

E-mail address :

15.1.2 Template for Pre-Bid Queries

S. No.	Page No.	Section (Name & No.)	Statement as per RFP	Statement as per MSP	Justification for query (if any)

15.1.3 Template for Board Resolution or Power of Attorney

[To be executed on stamp paper of appropriate value]

Know all men by these presents, We, *[Insert full legal name of the bidding entity]*, having registered office at *[Insert registered office address]* (hereinafter referred to as the "Principal") do hereby constitute, nominate, appoint and authorize *[Insert full name of authorized signatory]* son of *[Insert father's name]* presently residing at *[Insert address of authorized signatory]* who is presently employed with us and holding the position of *[Insert position / designation of the authorized signatory]* as our true and lawful attorney (hereinafter referred to as the "Authorized Attorney") to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to the submission of our proposal in response to the RFP bearing number ______ for **'Selection of Managed Service Provider (MSP) for providing Cloud services to MAHARASHTRA REMOTE SENSING APPLICATION CENTRE (MRSAC) Under MahaBHUMI Project of Govt. of Maharashtra for DC and DR for 5 years'** dated ______, including but not limited to signing and submission of all applications, proposals and other documents and writings, participating in pre-Bid and other conferences and providing information/ responses to the **MAHARASHTRA REMOTE SENSING APPLICATION CENTRE** (hereinafter referred to as the "MRSAC"), representing us in all matters before the MRSAC, signing and execution of all contracts and undertakings/ declarations consequent to acceptance of our Proposal and generally dealing with the MRSAC in all matters in connection with or relating to or arising out of our Proposal for the said assignment and/ or upon award thereof to us till the execution of appropriate Agreement/s with the MRSAC.

AND, we do hereby agree to ratify and confirm all acts, deeds and things lawfully done or caused to be done by our said Authorized Attorney pursuant to and in exercise of the powers conferred by this deed of Power of Attorney and that all acts, deeds and things done by our said Authorized Attorney in exercise of the powers hereby conferred shall always be deemed to have been done by us.

IN WITNESS THEREOF WE, ____________________________________ THE ABOVE-NAMED PRINCIPAL

HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS DAY OF ...., 2024

For_______________

(Signature, name, designation and address)
[Please put company seal if required]
[Notarize the signatures]

Witness 1:	Witness 2:
Name:	Name:
Designation:	Designation:
Address:	Address:
Signature:	Signature:

15.2 Instructions for Technical Bid Document Format

15.2.1 Technical Bid Cover Letter (MSP Company letter head)

[Date]

To

MRSAC Name and Address

Dear Sir,

Request for Proposal for Selection of Managed Service Provider MSP for procurement of Cloud services to MRSAC under MahaBHUMI Project of Govt. of Maharashtra for DC and DR for 5 years

Ref: Tender No: <No> Dated <DD / MM / YYYY>

Having examined the bid document, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the services for providing cloud services to host MahaBHUMI Project application of MRSAC as required and outlined in the RFP.

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

We undertake, if our proposal is accepted, to provide all the services put forward in this RFP or such features as may subsequently be mutually agreed between us and MRSAC.

We agree for unconditional acceptance of all the terms and conditions set out 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 bid and it shall remain binding upon us with full force and virtue, until within this period a formal agreement is prepared and executed. This bids response, together with your written acceptance thereof in your notification of award, shall constitute a binding agreement 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 to MRSAC is true, accurate, and complete. This proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead MRSAC as to any material fact.

We agree that you are not bound to accept the lowest or any bid response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products / service specified in the bid response without assigning any reason whatsoever.

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

Signature of Authorized Signatory (With official seal)

Name :

Designation :

Address : Telephone & Fax : E-mail address :

15.2.2 Checklist for the documents to be submitted

Technical Proposal (Packet A)

S. No	Documents Required	Page No. in the offer
1.	Brief Summary of the services offered	
2.	Project Management and Implementation Methodology	
3.	Migration Plan and Methodology	
4.	MSPs' compliance with the Technical Bill of Material (to be provided by the MSP as per Annexure II Section 14	
5.	Technical Brochures / Documents / Manuals from OEM containing the list of functionalities as mentioned in Annexure II Section 14	
6.	Clear articulation and description of the design and technical solution and various components including details of the operating System and other software Proposed	
7.	Details of Resources Proposed	
8.	Extent of compliance to the scope of work	
9.	Maintenance and support for proposed Solution	
10.	Risk Mitigation Plan	
11.	Strength of the MSP to provide services with examples of case studies of similar solutions implemented for past clients	
12.	Approach and Methodology of management of SLA requirements and articulate how SLA requirements would be adhered.	
13.	Other Documents (as per requirements of the bid)	

15.2.3 <u>Format for citations for MSPs Experience</u>

S. No.	Item	MSP's Response
1	Name of MSP entity	
2	Assignment Name	
3	Name of Client	
4	Name of the entity engaged in the Assignment	
5	Country	
6	Contact Details	
7	(Contact Name, Address, Telephone Number)	
8	Approximate Value of the Contract	
9	Duration of Assignment (months)	
10	Award Date (month / year)	
11	Completion Date (month / year)	
12	Narrative description of the project	
13	Details of Work that defines the scope relevant to the Requirement	
14	Documentary Evidence	

15.2.4 <u>Format for citations for CSPs Experience</u>

S. No.	Item	CSP's Response
1	Name of CSP entity	
2	Assignment Name	
3	Name of Client	
4	Name of the entity engaged in the Assignment	
5	Country	
6	Contact Details	
7	(Contact Name, Address, Telephone Number)	
8	Approximate Value of the Contract	
9	Duration of Assignment (months)	
10	Award Date (month / year)	
11	Completion Date (month / year)	
12	Narrative description of the project	
13	Details of Work that defines the scope relevant to the Requirement	
14	Documentary Evidence	

16 Annexure II:

Bill of Material- FOR CLOUD

16.1 Bill of Material

Compute node with standard storage					
S No.	Items	vCPU	Memory RAM (GB)	OS Size SSD (GB)	UoM
1.	Windows Server 64 bit	8 Core	16	500	Per VM
2.	Windows Server 64 bit	8 Core	32	500	Per VM
3.	Windows Server 64 bit	8 Core	64	500	Per VM
4.	Windows Server 64 bit	16 Core	32	500	Per VM
5.	Windows Server 64 bit	16 Core	64	500	Per VM
6.	Windows Server 64 bit	16 Core	128	500	Per VM
7.	Windows Server 64 bit	32 Core	64	500	Per VM
8.	Windows Server 64 bit	32 Core	128	500	Per VM
9.	Windows Server 64 bit	32 Core	256	500	Per VM
10.	Windows Server 64 bit	64 Core	128	500	Per VM
11.	Windows Server 64 bit	64 Core	256	500	Per VM
12.	Windows Server 64 bit	64 Core	512	500	Per VM
18.1.2 Compute node with NVMe storage for OS					
S No.	Items	vCPU	Memory RAM (GB)	OS Size SSD (GB)	UoM
13.	Windows Server 64 bit	8 Core	16	500	Per VM
14.	Windows Server 64 bit	8 Core	32	500	Per VM
15.	Windows Server 64 bit	8 Core	64	500	Per VM
16.	Windows Server 64 bit	16 Core	32	500	Per VM
17.	Windows Server 64 bit	16 Core	64	500	Per VM
18.	Windows Server 64 bit	16 Core	128	500	Per VM
19.	Windows Server 64 bit	32 Core	64	500	Per VM

20.	Windows Server 64 bit	32 Core	128	500	Per VM
21.	Windows Server 64 bit	32 Core	256	500	Per VM
22.	Windows Server 64 bit	64 Core	128	500	Per VM
23.	Windows Server 64 bit	64 Core	256	500	Per VM
24.	Windows Server 64 bit	64 Core	512	500	Per VM

18.1.3 Storage Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
25.	Disk Storage (Block)	Primary storage for data	Per 1 TB
26.	Disk Storage (File)	Primary storage for data	Per 1 TB
27.	NVMe SSD Storage	NVMe storage with 50K IOPS	Per 1 TB
28.	Backup Storage	Backup Storage in Object Store	Per 1 TB

18.1.4 Network Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
29.	Virtual Firewall 1Gbps throughput + IPS+IDS features - VM level and Subnet level	Allow / Deny inbound & outbound traffic	Per Firewall
30.	Virtual Server Load Balancer 1Gbps throughput	Load balance applications and for failover	Per VLB
31.	Virtual WAF 1Gbps throughput	Dedicated WAF to protect web application from external vulnerabilities	Per Gbps
32.	Content Delivery Network	For copying data to multiple locations	Per GB
33.	Unmetered Internet Bandwidth – Primary Site (independent of down / up data size)	100 Mbps	Per 10 Mbps
34.	Internet Bandwidth – DRs	Internet bandwidth of 50 Mb / s	Per 10 Mbps
35.	Site to Site VPN	VPN connections	Per connection
36.	Point to Site VPN	VPN connections	Per connection
37.	Public IP v4	To provide IP address for Applications.	Package of 16
38.	Networking Monitoring Dashboard / Monitoring tool - Visualize CPU, Server, Memory, Disk, Utilization, Raise alarm for threshold bridge	Visualising CPU, Server, Memory, Disk etc	Contract period (60 months)
39.	Caching Services	Caching	Per GB

18.1.5 Security Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
40.	SIEM solution with log retention 90 days	To provide real-time analysis of security alerts generated by applications and network hardware.	Per 500 EPS
41.	DDOS	Blocking and absorbing malicious spikes in network traffic and application usage caused by DDoS attacks, while allowing legitimate traffic to flow unimpeded.	Per 100 Mbps
42.	Domain SSL wildcard	Public key certificate which can be used with multiple sub-domains of a domain. The principal use is for securing web sites with HTTPS.	Per domain

43.	Anti-Virus with centralized Management	To protect your business systems from viruses and other threats.	Per VM
18.1.6 Other Components			
S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
44.	Memory	8 GB	Per 8 GB
45.	HDD	Hard disk	Per 5GB
46.	NVMe SSD	NVMe SSD	Per 5GB
47.	vCPU	No of cores	Per vCPU
48.	Postgres Enterprise license with post GIS	Managed DB services	Per month

17 Annexure III

17.1 Commercial Bid Declaration

Date: dd / mm / yyyy

To

MRSAC,

Address

Sub: Request for Proposal for Selection of Managed Service Provider MSP for procurement of Cloud services to MRSAC under MahaBHUMI Project of Govt. of Maharashtra for DC and DR for 5 years

Ref: Tender No: <No> Dated <DD / MM / YYYY>

Dear Sir,

We, the undersigned MSP, having read and examined in detail all the bidding documents in

respect of "Request for Proposal for Selection of Managed Service Provider MSP for procurement of Cloud services to MRSAC under MahaBHUMI Project of Govt. of Maharashtra for DC and DR for 5 years" do hereby propose to provide services as specified in the Bid Document referred above.

i. PRICE AND VALIDITY

All the prices mentioned in our proposal are in accordance with the terms as specified in the Tender documents. All the prices and other terms and conditions of this proposal are valid for entire contract duration.

We hereby confirm that our proposal prices exclude all taxes. Taxes may be paid as applicable.

We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other corporate Tax in altercated under the law, we shall pay the same.

ii. DEVIATIONS

We declare that all the services shall be performed strictly in accordance with the Bid Documents and there are no deviations except for those mentioned in Pre-Qualification Envelope, irrespective of whatever has been stated to the contrary anywhere else in our bid.

iii. QUALIFYING DATA

We confirm having submitted the information as required by you in your Instruction to CSP / MPSs. In case you require any other further information / documentary proof in this regard before evaluation of our proposal, we agree to furnish the same in time to your satisfaction.

iv. BID PRICE

We declare that our Bid Price is for the entire scope of the work as specified in the Bid Document. The bid price at which the contract is awarded shall hold good for entire tenure of the contract. These prices are indicated in the subsequent sub-sections of this Section.

v. CONTRACT PERFORMANCE GUARANTEE BOND

We hereby declare that in case the contract is awarded to us, we shall submit the Performance Bank Guarantee in the form prescribed in the Bid Document.

We hereby declare that our proposal is made in good faith, without collusion or fraud and the information contained in the Tender is true and correct to the best of our knowledge and belief. We understand that our proposal is binding on us and that you are not bound to accept any proposal you receive. We confirm that no technical deviations are attached here with this commercial offer.

Thanking you, Yours faithfully,

(Signature of the authorised signatory)
Name:
Designation
Address:
Seal:
Date:
Place:

17.2 Commercial Proposal:

17.2.1 Best Price Offer Letter Format

On Rs. 500/- Stamp Paper duly notarized by notary with red seal and registration number

Date: dd / mm / yyyy

To

MRSAC Official and Address

Sub: Request for Proposal for Selection of Managed Service Provider MSP for procurement of Cloud services to MRSAC under MahaBHUMI Project of Govt. of Maharashtra for DC and DR for 5 years"

Ref: Tender No: <No> Dated <DD / MM / YYYY>

Dear Sir,

"I / We (full name in capital letters, starting with

surname), the Managing Partner / Managing Director / Holders of the Business / Manufacturer / Authorized Dealer, for the establishment / firm / registered company, name herein below, do hereby, state and declare that I / We ………………………………………………………………. whose names are given herein below in details with the addresses have not filled in this tender under any other name or under the name of any other establishment / firm or otherwise, nor are we in any way related or concerned with any establishment / firm or any other person, who have filled in the tender for the aforesaid work."

"I / We do hereby further undertake that; we have offered the best prices for the subject supply / work as per the present market rates. Further, we have filled in the accompanying tender with full knowledge of the above liabilities and therefore we will not raise any objection or dispute in any manner relating to any action, including forfeiture of deposit and blacklisting, for giving any information which is found to be incorrect and against the instruction and direction given in this behalf in this tender.

I / We further agree and undertake that in the event, if it is revealed subsequently after the allotment of work / contract to me / us, that any information given by me / us in this tender is false or incorrect, I / We shall compensate MRSAC for any such losses or inconvenience caused to the corporation in any manner and will not raise any claim for such compensation on any ground whatsoever, I / We agree and undertake that I / We shall not claim in such case any amount, by way of damages or compensation for cancellation of the contract given to me / us or any work assigned to me / us or is withdrawn by the Corporation.

(Signature of the Authorized Signatory with Full Name & Rubber Stamp)

17.3 Commercial Bid Format & Instructions

The MSP has to quote the rate for the Bill of Quantity available in Annexure II Section 14. The MSP must share per unit pricing for each of the components listed in Annexure II Section 14

13. The rates quoted are to be specified in "Per-Item-Per unit" basis. Any tools / software used during the project and support must be clearly discussed and approved with MRSAC and the cost of the same must be solely incurred by the MSP.

It is mentioned that the Commercial Bid evaluation would be done based on the Commercial sheet. The MSP has to provide per item per unit rates for Compute, Storage, Network, Security, Monitoring, Usage, Disaster recovery Support, Exit management, Business Continuity Planning, Project planning and other requirements. The cost based on the usage per item per unit shall remain uniform for the entire duration of the contract and shall also remain uniform when scaling up and scaling down of the requirements.

Other Requirements

a. All the prices are to be entered in Indian Rupees ONLY

b. The above charges must include Cloud DR provisioning (i.e., provisioning of required resource on DR site of Cloud)

c. The MSP needs to account for all Out-of-Pocket expenses due to Boarding, Lodging and other related items.

d. Prices indicated in the schedules shall be inclusive of all taxes, Levies, duties etc. During the payment stage, MRSAC reserves the right to ask the MSP to submit proof of payment against any of the taxes, duties, levies indicated.

17.4 Commercial Bid Format

The MSP is required to provide costs as per the following tables. The price in the commercial bid is excluding taxes. Government of India specified taxes would be applied to the price bid.

i. Managed services price bid value (MSPBV)

Compute node with standard storage					
S No.	Items	vCPU	Memory RAM (GB)	OS Size SSD (GB)	UoM
1.	Windows Server 64 bit	8 Core	16	500	Per VM
2.	Windows Server 64 bit	8 Core	32	500	Per VM
3.	Windows Server 64 bit	8 Core	64	500	Per VM
4.	Windows Server 64 bit	16 Core	32	500	Per VM
5.	Windows Server 64 bit	16 Core	64	500	Per VM
6.	Windows Server 64 bit	16 Core	128	500	Per VM
7.	Windows Server 64 bit	32 Core	64	500	Per VM
8.	Windows Server 64 bit	32 Core	128	500	Per VM
9.	Windows Server 64 bit	32 Core	256	500	Per VM
10.	Windows Server 64 bit	64 Core	128	500	Per VM
11.	Windows Server 64 bit	64 Core	256	500	Per VM
12.	Windows Server 64 bit	64 Core	512	500	Per VM
Compute node with NVMe storage for OS					
S No.	Items	vCPU	Memory RAM (GB)	OS Size SSD (GB)	UoM
13.	Windows Server 64 bit	8 Core	16	500	Per VM
14.	Windows Server 64 bit	8 Core	32	500	Per VM
15.	Windows Server 64 bit	8 Core	64	500	Per VM
16.	Windows Server 64 bit	16 Core	32	500	Per VM
17.	Windows Server 64 bit	16 Core	64	500	Per VM
18.	Windows Server 64 bit	16 Core	128	500	Per VM
19.	Windows Server 64 bit	32 Core	64	500	Per VM
20.	Windows Server 64 bit	32 Core	128	500	Per VM

21.	Windows Server 64 bit	32 Core	256	500	Per VM
22.	Windows Server 64 bit	64 Core	128	500	Per VM
23.	Windows Server 64 bit	64 Core	256	500	Per VM
24.	Windows Server 64 bit	64 Core	512	500	Per VM

Storage Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
25.	Disk Storage (Block)	Primary storage for data	Per 1 TB
26.	Disk Storage (File)	Primary storage for data	Per 1 TB
27.	NVMe SSD Storage	NVMe storage with 50K IOPS	Per 1 TB
28.	Backup Storage	Backup Storage in Object Store	Per 1 TB

Network Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
29.	Virtual Firewall 1Gbps throughput + IPS+IDS features - VM level and Subnet level	Allow / Deny inbound & outbound traffic	Per Firewall
30.	Virtual Server Load Balancer 1Gbps throughput	Load balance applications and for failover	Per VLB
31.	Virtual WAF 1Gbps throughput	Dedicated WAF to protect web application from external vulnerabilities	Per Gbps
32.	Content Delivery Network	For copying data to multiple locations	Per GB
33.	Unmetered Internet Bandwidth – Primary Site (independent of down / up data size)	100 Mbps	Per 10 Mbps
34.	Internet Bandwidth – DRs	Internet bandwidth of 50 Mb / s	Per 10 Mbps
35.	Site to Site VPN	VPN connections	Per connection
36.	Point to Site VPN	VPN connections	Per connection
37.	Public IP v4	To provide IP address for Applications.	Package of 16
38.	Networking Monitoring Dashboard / Monitoring tool - Visualize CPU, Server, Memory, Disk, Utilization, Raise alarm for threshold bridge	Visualising CPU, Server, Memory, Disk etc	Contract period (60 months)

39.	Caching Services	Caching	Per GB

Security Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
40.	SIEM solution with log retention 90 days	To provide real-time analysis of security alerts generated by applications and network hardware.	Per 500 EPS
41.	DDOS	Blocking and absorbing malicious spikes in network traffic and application usage caused by DDoS attacks, while allowing legitimate traffic to flow unimpeded.	Per 100 Mbps
42.	Domain SSL wildcard	Public key certificate which can be used with multiple sub-domains of a domain. The principal use is for securing web sites with HTTPS.	Per domain
43.	Anti-Virus with centralized Management	To protect your business systems from viruses and other threats.	Per VM

Other Components

S. No	Items with minimum spec	Description	UoM (Unit of Measurement)
44.	Memory	8 GB	Per 8 GB
45.	HDD	Hard disk	Per 5GB
46.	NVMe SSD	NVMe SSD	Per 5GB
47.	Vcpu	No of cores	Per vCPU
48.	Postgres Enterprise license with post GIS	Managed DB services	Per month

ii. Cloud resources price bid value

This is to discover unit prices so that MRSAC can pay on a pay-as-you go during the consumption of cloud services. The Price quote will be valid throughout the contract duration. This quote is only for commercial evaluation. The actual payment will be as per usage and as defined in the payment terms of this RFP. Actual requirements of line items in terms of quantity and usage hours will be as per MRSAC requirement and payment would be made for the same. The cloud resources price bid value for assessment as given in the table above shall be used to arrive at the total price for comparative bid assessment.

Signature valid ✓

Digitally signed by PRANOTI VILAS
BULKUNDE
Date: 2024.08.08 17:08:34 IST
Location: Maharashtra-MH