RAILTEL CORPORATION OF INDIA LIMITED

(A Govt. of India Undertaking)

Expression of Interest for Selection of Partner from Empanelled Business Associate for EXCLUSIVE PRE-BID TEAMING ARRANGEMENT

For

"Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development"

EOI No: RCIL/WR/MUMBAI/Mktg/23-24/005 dated 23th Nov, 2023

EOI NOTICE

RailTel Corporation of India Ltd,
Western Railway Microwave Complex, Senapati bapat Marg,
Mahalaxmi, Mumbai – 400013

EOI Notice No: RCIL/WR/MUMBAI/Mktg/23-24/005 dated 23th Nov, 2023

RailTel Corporation of India Ltd., (here after referred to as "RailTel") invites EOIs from RailTel's Empaneled Partners for the selection of suitable partner as Exclusive pre bid teaming arrangement for "Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development".

The details are asunder:

1	Last date for submission of Technical Packet against EOIs by bidders	28th Nov 2023 at 12:00 Hours
2	Opening of Technical Bid of EOIs	28th Nov 2023 at 12:30 Hours
3	Number of copies to be submitted for scope of work	One
4	EOI fees inclusive tax(Non-refundable)	Rs. 5900/-
5	EMD for Pre-Bid Arrangement	Rs. 400000/-

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 of payment to the below mentioned officers along with the proposal.

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

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

1. Level 1
Contact Name : Sh. Viplovnath Mishra
Designation : Deputy General Manager/ Marketing
E-Mail Address : viplovmishra@railtelindia.com
Mobile No : +91- 9004444124

2. Level 2
Contact Name : Sh. Santosh Parage
Designation : General Manager/ Marketing
E-Mail Address : santosh.parage@railtelindia.com
Mobile No : +91- 7020906278

Note:

1. Empanelled partners are required to submit soft copy of technical packet through an e-mail at **eoi.wr@railtelindia.com** duly signed by Authorized Signatories with Company seal and stamp.
2. The EOI response is invited from eligible **Empanelled Partners of RailTel only.**
3. All the document must be submitted with **proper indexing** and **page no**.
4. This is an **exclusive pre RFP partnership arrangement with empanelled business associate of RailTel for participating in the end customer RFP**. 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 in this EOI for pre-bid teaming arrangement (before and after submission of bid to end customer organization by RailTel).This undertaking has to be given with this EOI Response.
5. Partner can submit their response as an individual organization. Consortium is not permitted. The Bidder has to be an empanelled partner of RailTel.
6. **Transfer and Sub-letting**. The Business Associate has no right to give, bargain, sell, assign or sublet or otherwise dispose of the Contractor 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.
7. All Bidders to sign and stamp RailTel's EOI and its corrigendums implying acceptance of all terms and conditions as mentioned and submit the same along with their Bids.

1. Introduction about RailTel

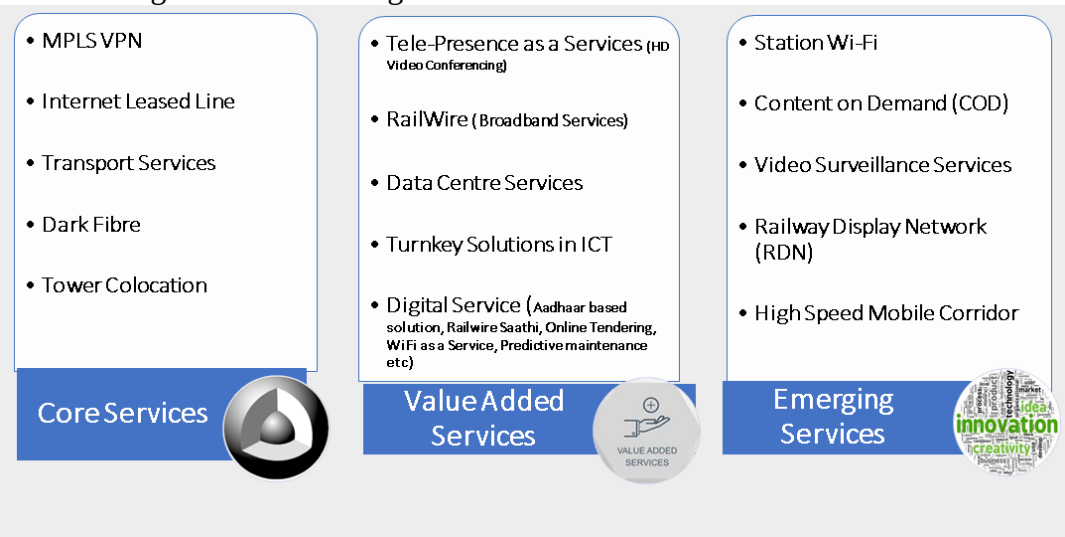
RailTel Corporation of India Limited (RailTel), is a Mini Ratna Government of India undertaking under the Ministry of Railways. The Corporation was formed in Sept 2000 with the objectives to create nationwide Broadband Telecom and Multimedia Network in all parts of the country, to modernize Train Control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

RailTel has approximately 65000+ kms of OFC along the protected Railway tracks. The transport network is built on high capacity DWDM and an IP/ MPLS network over it to support mission critical communication requirements of Indian Railways and other customers. RailTel has Tier-III Data Center in Gurgaon and Secunderabad hosting / collocating critical applications. RailTel is also providing Telepresence as a Service (TPaaS), where a High-Definition Video Conference facility bundled with required BW is provided as a Service.

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

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

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



a) Carrier Services

- National Long Distance: Carriage of Inter & Intra -circle Voice Traffic across India

using stateof 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/BTSof 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 yourfingertips 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.

d) National Long Distance:

Carriage of Inter & Intra -circle Voice Traffic across India using stateof 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/BTSof Telco's

e) 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 tobe productive specially during this pandemic situation.

f) 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. 4,68,000 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 Tender floated by end Customer organization for "Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO" with tender Ref. No. 05/CIDCO/SD/SM/2023-24 dated 31-Oct-2023.

RailTel invites EOIs from RailTel's Empanelled Partners for the selection of suitable partner for participating in above mentioned work for the agreed scope work. The empanelled partner is expected to have excellent execution capability and good understanding customer local environment.

3. Scope of Work

The scope of work will be as mentioned in the end Customer organization Tender for "Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO" with tender Ref. No. 05/CIDCO/SD/SM/2023-24 dated 31-Oct-2023 with latest and all amendment/ Corrigendum/ Clarifications/ Documents**.**

The broad scope of deliverables is provided below for reference: -
Redesign and Revamping of Website-The CIDCO website will provide a secure unified access point in the form of a web-based user interface and will be redesigned to publish official information about CIDCO and integrate with other CIDCO's online service platforms. The website should follow GIGW guidelines. This website shall be a source of all information, forms, and payments of different services, etc. for customers and shall act as and operate the required functions.

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

In case of any discrepancy or ambiguity in any clause / specification pertaining to scope of work area, the RFP and corrigendum/addendum released by 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.)

Business associate can participate as a sole bidder and no consortium is permitted.

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.

4. Response to EOI guidelines

4.1 Language of Proposals

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

4.2 RailTel's Right to Accept/Reject responses

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

4.3 EOI response Document

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

All pages of the documents shall be signed by the bidder including the closing page in token of his having 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 a period of 120 days from the date Bid submission date issued by the end Customer organization for which bid is going to submit.

4.5 Bid Earnest Money (EMD)

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

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

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

4.5.4 **Return of EMD for successful Business Associate:** Earnest Money Deposit and Integrity Pact 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. 4.6) from BusinessAssociate whichever is later.

4.5.5 **Forfeiture of EMD and or Penal action asper EMD Declaration:**

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

4.5.5.2 In case of non-submission of SD/PBG (as per clause no. 4.6) lead to forfeiture of EMD if applicable and Integrity Pact and or suitable action as prescribed in the EMD Declaration shall be initiated as applicable.

4.5.6 Having participated with another party/consortium apart from RailTel in RailTel's end customer Tender

4.6 Security Deposit / Performance Bank Guarantee (PBG)

4.6.1 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.

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

4.7 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.

4.8 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.

4.9 Details of Financial bid for the above referred tender

Business Associate meeting eligibility criteria and clearing the technical evaluation will be selected for exclusive pre-bid arrangement for optimizing technical and commercial solution so that most winnable solution is submitted to end customer.

In case if there are Two or more Business Associate meeting eligibility criteria and clearing technical evaluation criteria, then price bid will be sought from these Sole bidder in the second stage for the given scope of the work and Sole bidder with overall lowest (L1) offer will be selected for exclusive pre bid arrangement for optimizing technical and commercial solution.

The final bid for the tender will be prepared jointly with the selected Business Associate so that the optimal bid can be put with a good chance of winning the Tender.

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 theprice or substance of the EOI response shall be sought, offered or permitted.

4.11 Period of Association/Validity of Agreement

RailTel will enter into a pre-bid agreement with selected bidder with detailed Terms and conditions.

5. Eligibility Criteria for Bidding Business Partner of RailTel

S No	Particulars	Criteria for Tender Package (Mandatory Compliance & Document Submission)
A)	**Financial Conditions**	
i)	Sole bidder members should be registered under Companies Act, 1956 or Companies Act 2013 or as amended and should have at least 3 years of operations in India as on bid submission date.	1. Certificate of Incorporation 2. GST Registration 3. PAN Card
ii)	Sole Participating partner should have average annual turnover of at least INR 25 Cr. for last three years (FY 20-21, 21-22, 22-23).	Turnover Certificate issued by the Chartered Accountant for sole bidders. Certificate should contain UDIN no. issued by ICAI
iii)	Sole bidder should also have a positive net worth & be profitable in each of the last 3 financial years (i. e. FY 20-21, 21-22, 22-23).	Positive Net Worth and Profitability Certificate issued by the CA for the last three financial years (i. e. FY 20-21, 21-22, 22-23). Certificate should contain UDIN no. issued by ICAI.
B)	**Technical Conditions**	
iv)	Experience of work for IT related services involving Design Development, Implementation and Maintenance of an official Website implementation or maintenance of cloud infrastructure service in Govt./Semi. Govt. sectors / PSUs in last 5 years as on bid submission date: 1. One work order/Contract costing not less than Rs. 3.4 Crores OR 2. Two work orders/Contracts costing not less than Rs. 2.5 Crores each OR 3. Three work orders/Contracts costing not less than Rs. 1.7 Crores each	PO Copies along with Self certificate for completion
v)	**Certifications:** 1) ISO 9001:2015 2) ISO 27001:2013	Copies of Certificates (priority will be given to higher level of certifications)
vi)	The bidder must have on its roll a minimum of 50 qualified staff	Declaration on letter head

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 emailAddress	
4.	Full address, telephone and fax numbers, and email addresses of the officeof 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	
8.	PAN Number	

7. Evaluation Criteria

7.1 The Business Associates are first evaluated on the basis of the Eligibility Criteria as per clause 5 above.
7.2 The Business Associate qualifying the Eligibility criteria will be selected for exclusive pre-bid arrangement for optimizing technical and commercial solution so that most winnable solution is submitted to end customer.
7.3 In case if there are two or more Sole bidders meeting eligibility criteria then the price bids will be sought from these Sole bidders in the second stage for the given scope of the work and Sole bidder with overall lowest (L1) offer will be selected for exclusive pre bid arrangement for optimizing technical and commercial solution.
7.4 RailTel reserves the right to accept or reject the response against this EOI, without assigning any reasons. The decision of RailTel is final and binding on the participants. The RailTel evaluation committee will determine whether the proposal/ information is complete in all respects and the decision of the evaluation committee shall be final. RailTel may at its discretion assign lead factor to the Business associate as per RailTel policy for shortlisting partner against this EOI.
7.6 All General requirements mentioned in the Technical Specifications are required to be complied. The solution proposed should be robust and scalable.

8 Withdrawal of Bids

A Bidder wishing to withdraw its bid shall notify to RailTel by e-mail prior to the deadline prescribed for bid submission. The notice of withdrawal shall be addressed to RailTel at the address named in the Bid Data Sheet, and bear the Contract name, the <Title> and < Bid No.>, and the words "Bid Withdrawal Notice." Bid withdrawal notices received after the bid submission deadline will be ignored, and the submitted bid will be deemed to be a valid submitted bid.

No bid can be withdrawn in the interval between the bid submission deadline and the expiration of the bid validity period specified in the Bid Data Sheet. Withdrawal of a bid during this interval may result in the forfeiture of the Bidder's EMD.

9 Evaluation Process

The evaluation process of the bid proposed to be adopted by RailTel is indicated in this section. The purpose of this section is to provide the Bidder an idea of the evaluation process that RailTel may adopt.

RailTel shall appoint a Bid Evaluation Committee (BEC) to scrutinize and evaluate the technical and commercial bids received. The BEC will examine the Bids to determine whether they are complete, responsive and whether the bid format conforms to the bid requirements. RailTel may waive any informality or non-conformity in a bid which does not constitute a material deviation according to RailTel.

The bid prices should not be mention in any part of the bid other than the Commercial Bid. Any attempt by a bidder to influence the bid evaluation process may result in the rejection of Bid and forfeiture of EMD.

10 Performance Bank Guarantee

The Bidder shall at his own expense, deposit with RailTel, an unconditional and irrevocable Performance Bank Guarantee (PBG) from nationalized banks as per the format given in this bid, payable on demand, for the due performance and fulfillment of the contract by the Bidder.

This Performance Bank Guarantee will be submitted within 30 days of the notification of award of the contract/ Letter of Acceptance (LOA) issuance whichever is earlier. If PBG is not submitted within this time frame a delayed PBG penalty will be attracted. Post 30 days and upto 60 days from date of notification of award of the contract/ Letter of Acceptance (LOA) issuance a penalty at 15% per annum interest of LOA amount will be levied as delayed PBG penalty and this penalty will be deducted from the Invoices & EMD of the Bidder. After these 60 days if PBG is not submitted then it will be assumed that the Bidder is not interested in submitting PBG and the Amount of PBG along with the delayed PBG penalty calculated will be retained from Invoices & EMD of the Bidder. Non submission of PBG can also lead to cancellation of contract and the decision with respect to whether, to retain the PBG Amount and penalty from Invoices & EMD or cancellation of contract, will be at the sole discretion of RailTel. In the event of cancellation of contract EMD will be forfeited. If PBG is retained from Invoices & EMD then

the PBG Amount only and not the penalty attracted will be paid to the Bidder in such a case post the contract period plus three months(expected PBG validity date) are over after deducting any applicable deductions (eg: Poor service, etc).

This Performance Bank Guarantee will be for an amount equivalent to 3% of the total contract value. All charges whatsoever such as premium, commission, etc. with respect to the Performance Bank Guarantee shall be borne by the Bidder. The Performance Bank Guarantee format can be found in this document.

The Performance Bank Guarantee may be discharged/ returned by RailTel upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the Performance Bank Guarantee.

In the event of the Bidder being unable to service the contract for whatever reason, RailTel would invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of RailTel under the Contract in the matter, the proceeds of the PBG shall be payable to RailTel as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract. RailTel shall notify the Bidder in writing of the exercise of its right to receive such compensation within 30 days, indicating the contractual obligation(s) for which the Bidder is in default.

The 30days' notice period shall be considered as the 'Cure Period' to facilitate the Implementation Agency to cure the breach. The PBG shall be invoked only if the breach is solely attributable to the bidder and the bidder fails to rectify the breach within the 'Cure Period'.

RailTel shall also be entitled to make recoveries from the Bidder's bills, performance bank guarantee, or from any other amount due to the Bidder, the equivalent value of any payment made to the Bidder due to inadvertence, error, collusion, misconstruction or misstatement.

11 Rights to Terminate the Process

RailTel may terminate the bid process at any time and without assigning any reason. RailTel 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 RailTel. The Bidder's participation in this process may result in RailTel selecting the Bidder to engage in further discussions and negotiations towards execution of a contract. The commencement of such negotiations does not, however, signify a commitment by RailTel to execute a contract or to continue negotiations. RailTel may terminate negotiations at any time without assigning any reason.

12. 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 and upon submission of correct Tax Invoices as per statutory norms.

8.3 The Payments received from end customer will be disbursed scope wise to the selected BA. The BA selected for a particular scope will receive payments once end customer releases payments for the specific part

13 SLA

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

Note:

1. **Depending on RailTel's business strategy RailTel may choose to work with Partner who is most likely to support in submitting a winning bid**
2. **All Documents and requirements like EMD, Tender Fees, PBG, Contract Agreement to be shared/executed Back to Back as per the end customer RFP/Tender**
3. **In case of any discrepancy or ambiguity in any clause /specification pertaining to scope of work area, the RFP released by end customer organization shall supersede and will be considered sacrosanct. (All associated clarifications, response to queries, revisions, addendum and corrigendum, associated prime service agreement (PSA)/ MSA/ SLA also included.)**
4. **All clauses such as cost involved, payment terms, SLA, lock in period, validity, esclations, penalties, etc will be back to back as per CIDCO RFP.**

Annexure 1: Format for COVERING LETTER (to be submitted by sole bidder)

COVERING LETTER (To be on company letter head)

EoI Reference No: _____ Date:_____

To,

RailTel Corporation of India Ltd.
Western Railway Microwave complex,
Senapati Bapat Marg, Mahalaxmi, Mumbai – 400013

Dear Sir,

SUB: Participation in the EoI process

Having examined the Invitation for EoI document bearing the reference number _____ Dt. _____ 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:
Signature:
Seal of the Organization:

Annexure 2: Format for Self-Certificate & Undertaking (to be submitted by sole bidder)

Self-Certificate (To be on company letter head)

EoI Reference No: _____ Date:_____

To,

RailTel Corporation of India Ltd.
Western Railway Microwave complex,
Senapati Bapat Marg, Mahalaxmi, Mumbai – 400013

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 sole bidder after the receipt of corresponding payment from end customer by RailTel. Further we understand that in case selected sole bidder 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 sole bidder.
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 certify that any services, equipment and materials to be supplied are produced in eligible source country complying with OM/F. No. 6/18/2019 dated 23rd July 2020 issued by DoE, MoF.
6. We hereby undertake to work with RailTel as per end customer's RFP terms and conditions. We confirm to submit all the supporting documents constituting/ in compliance with the Criteria as required in the end customer's RFP terms and conditions like technical certificates, OEM compliance documents.
7. We understand and agree that RailTel is intending to select a sole bidder who is willing to accept all terms & conditions of end customer organization's RFP for the agreed scope of work. RailTel will strategies to retain scope of work where RailTel has competence.

8. We hereby agree to submit that in case of being selected by RailTel as sole bidder 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.

9. We hereby undertake to sign Pre Bid Agreement, Pre-Contract Integrity Pact and Non-Disclosure Agreement with RailTel on a non-judicial stamp paper of Rs. 100/- in the prescribed Format.
10. We undertake that we will not submit directly or indirectly out bids and techno-commercial solution/association with any other organization once selected in this EOI for pre-bid teaming arrangement (before and after submission of bid to end customer organization by RailTel)

Authorized Signatory Name:
Designation:
Signature:
Seal of the Organization:

Annexure 3: Undertaking for not Being Blacklisted/Debarred (to be submitted by sole bidder)

EoI Reference No: _____ Date:_____

To,

RailTel Corporation of India Ltd.
Western Railway Microwave complex,
Senapati Bapat Marg, Mahalaxmi, Mumbai – 400013

Dear Sir,

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.

Authorized Signatory Name:
Designation:
Signature:
Seal of the Organization:

Annexure 4: Format of Affidavit (to be submitted by sole bidder)

FORMAT FOR AFFIDAVIT TO BE UPLOADED BY SOLE BIDDER ALONG WITH THE EOI DOCUMENTS

(To be executed in presence of Public notary on non-judicial stamp paper of the value of Rs. 500/-. 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._____ Dt. _____ 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 SIGNAURE OF THE ADVOCATE

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: Draft Non-Disclosure Agreement

(To be submitted on a Rs. 100 Stamp Paper)

This Non-Disclosure Agreement ("Non-Disc") is made and entered into _____ day of _____ month _____ year (effective date) by and between _____ ("Department") and _____ ("Company"). Whereas, Department and Company have entered into an Agreement ("Agreement") _____ effective _____ for _____ and

Whereas, each party desires to disclose to the other party certain information in oral or written form which is proprietary and confidential to the disclosing party, ("CONFIDENTIAL INFORMATION").
NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein, the parties agree as follows:

1. **Definitions. As used herein:**
    a. The term "Confidential Information" shall include, without limitation, all information and materials, furnished by either Party to the other in connection with citizen/users/persons/customers data, products and/or services, including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic or optical media, and including all proprietary information, customer and prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, commercial or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to the disclosing party's data, computer database, products and/or services. Results of any tests, sample surveys, analytics, data mining exercises or usages etc. carried out by the receiving party in connection with the Department's information including citizen/users/persons/customers personal or sensitive personal information as defined under any law for the time being in force shall also be considered Confidential Information.
    b. The term, "Department" shall include the officers, employees, agents, consultants, contractors and representatives of Department.
    c. The term, "Company" shall include the directors, officers, employees, agents, consultants, contractors and representatives of Company, including its applicable affiliates and subsidiary companies.
2. **Protection of Confidential Information:** With respect to any Confidential Information disclosed to it or to which it has access, Company affirms that it shall:
    a. Use the Confidential Information as necessary only in connection with Project and in accordance with the terms and conditions contained herein;

b. Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential Information that the parties take to protect the confidentiality of its own proprietary and confidential information and that of its clients;
c. Not to make or retain copy of any commercial or marketing plans, citizen/users/persons/customers database, Bids developed by or originating from Department or any of the prospective clients of Department except as necessary, under prior written intimation from Department, in connection with the Project, and ensure that any such copy is immediately returned to Department even without express demand from Department to do so;
d. Not disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the express written consent of the other party; and
e. Return to the other party, or destroy, at Department's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately upon the earlier to occur of (i) expiration or termination of either party's engagement in the Project, or
(ii) the request of the other party therefore.
f. Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between Department and Company or the nature of services to be provided by the Company to the Department.

3. **Onus.** Company shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the foregoing exceptions.
4. **Exceptions.** These restrictions as enumerated in section 1 of this Agreement shall not apply to any Confidential Information:
    a. Which is independently developed by Company or lawfully received from another source free of restriction and without breach of this Agreement; or
    b. After it has become generally available to the public without breach of this Agreement by Company; or
    c. Which at the time of disclosure to Company was known to such party free of restriction and evidenced by documentation in such party's possession; or
    d. Which Department agrees in writing is free of such restrictions.
    e. Which is received from a third party not subject to the obligation of confidentiality with respect to such Information;
5. **Remedies.** Company acknowledges that

(a) any actual or threatened disclosure or use of the Confidential Information by Company would be a breach of this agreement and may cause immediate and irreparable harm to Department;

(b) Company affirms that damages from such disclosure or use by it may be impossible to measure accurately; and

(c) injury sustained by Department may be impossible to calculate and remedy fully. Therefore, Company acknowledges that in the event of such a breach, Department shall be entitled to specific performance by Company of Company's obligations contained in this Agreement. In addition, Company shall indemnify Department of the actual and liquidated damages which may be demanded by Department. Moreover, Department shall be entitled to recover all costs (including reasonable attorneys' fees) which it or they may incur in connection with defending its interests and enforcement of legal rights arising due to a breach of this agreement by Company.

6. **Need to Know.** Company shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know (and advise such employees of the obligations assumed herein), shall use the Confidential Information only for the purposes set forth in the Agreement, and shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of the disclosing party.
7. **Intellectual Property Rights Protection.** No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.
8. **No Conflict.** The parties represent and warrant that the performance of its obligations hereunder do not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.
9. **Authority.** The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.
10. **Dispute Resolution.** If any difference or dispute arises between the Department and the Company in connection with the validity, interpretation, implementation or alleged breach of any provision of this Agreement, any such dispute shall be referred appropriately to RailTel/ stakeholders/ partners/ patrons
    a. The arbitration proceedings shall be conducted in accordance with the (Indian) Arbitration and Conciliation Act, 1996 and amendments thereof.
    b. The place of arbitration shall be Mumbai.
    c. The arbitrator's award shall be substantiated in writing and binding on the parties.
    d. The proceedings of arbitration shall be conducted in English language.
    e. The arbitration proceedings shall be completed within a period of 180 days from the date of reference of the dispute to arbitration.
11. **Governing Law.** This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to the exclusive

jurisdiction of Courts and/or Forums situated at Mumbai, India only.

12. **Entire Agreement.** This Agreement constitutes the entire understanding and agreement of the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.
13. **Amendments.** No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.
14. **Binding Agreement.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.
15. **Severability.** It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.
16. **Waiver.** If either party should waive any breach of any provision of this Agreement, it shall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.
17. **Survival.** Both parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement shall survive till perpetuity even after any expiration or termination of this Agreement.
18. **Non-solicitation.** During the term of this Agreement and thereafter for a further period of two (2) years Company shall not solicit or attempt to solicit Department's employees and/or consultants, for the purpose of hiring/contract or to proceed to conduct operations/business similar to Department with any employee and/or consultant of the Department who has knowledge of the Confidential Information, without the prior written consent of Department. This section will survive irrespective of the fact whether there exists a commercial relationship between Company and Department.
19. **Term.** Subject to aforesaid section 17, this Agreement shall remain valid up to _____ years from the "effective date".

IN WITNESS HEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.

For Department

Name:

Title:

WITNESSES:

1. _____

_____

2. _____

_____

For Company

Name:

Title:

WITNESSES:

1. _____

_____

2. _____

_____

Annexure 6: Integrity Pact

(To be executed on Rs. 500/- Stamp Paper)

EoI Number: _____ Dated: _____

This Integrity Pact is made at on this _____ Day of _____ 2022

BETWEEN

RailTel Corporation of India Ltd (a Govt of India Enterprise under Ministry of Railways) having its registered office at Plate-A, 6th Floor, Office Block Tower-2,East Kidwai Nagar, New Delhi-110023and Regional Office at Western Railway Microwave Complex, Senapati Bapat Marg, Mahalaxmi, Mumbai – 400013, hereinafter referred to as "The Principal", which expression shall unless repugnant to the meaning or contract thereof include its successors and permitted assigns
AND
<Bidder Name> having its registered office at <Bidders Registered and Branch Address (if any)> hereinafter referred to as "The Bidder/ Contractor/ Concessionaire/ Consultant" and which expression shall unless repugnant to be meaning or context thereof include its successors and permitted assigns.

Preamble

Whereas, the Principal intends to award, under laid down organizational procedures contract/s for 'Procurement, Installation, Commissioning and Management of SDWAN for MSEDCL Field Offices up to Subdivision level'. The Principal values full compliance with all relevant laws of the land, rules of land, regulations, economic use of resources and of fairness/ transparency in its relations with its Bidder(s) and for Contractor(s)/Concessionaire(s)/Consultant(s).

And whereas in order to achieve these goals, the Principal will appoint an independent external Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the Principles mentioned above.

And whereas to meet the purpose aforesaid, both the parties have agreed to enter into this Integrity Pact (hereafter referred to as Integrity Pact) the terms and conditions of which shall also be read as integral part and parcel of the Tender documents and contract between the parties. Now, therefore, in consideration of mutual covenants stipulated in this pact, the parties hereby agree as follows and this pact witnesseth as under:-

Article – 1: Commitments of the Principal

1. The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principle:-
    a. No employee of the Principal, personally or through family members, will in connection with the Tender for, or the execution of a contract, demand take a promise for or accept for self or third person any material or immaterial benefit which the person is not legally entitled to.
    b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/ additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
    c. The Principal will exclude all known prejudiced persons from the process.
2. If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act or any other Statutory Acts or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions as per its internal laid down Rules/ Regulations.

Article – 2: Commitments of the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s)

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

a. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principals employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.
b. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission or bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.
c. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not commit any offence under the relevant IPC / PC. Act and other Statutory Acts; further the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not use improperly for purposes of completion or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship,

regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) of foreign origin shall disclose the name and address of the Agents/ representatives in India. If any similarly the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) of Indian Nationality shall furnish the name and address of the foreign principle, if any. Further details as mentioned in the 'Guidelines on Indian Agents of Foreign Suppliers' shall be disclosed by the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s). Further, all the payments made to the Indian Agent /Representative have to be Indian Rupees only.
e. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract. He shall also disclose the details of services agreed upon for such payments.
f. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.
g. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not bring any outside influence through any Govt. bodies/quarters directly or indirectly on the bidding process in furtherance of his bid.
h. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) who have signed a Integrity pact shall not approach the court while representing the matter to IEMs and shall wait for their decision in the matter.

Article – 3: Disqualification from tender process and exclusion from future contracts

1. If the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) before award or during execution has committed a transgression through a violation of any provision of Article-2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) from the tender process.
2. If the Bidder/Contractor/Concessionaire/Consultant has committed a transgression through a violation of Article-2 such as to put his reliability or credibility into question, the Principal shall be entitled to exclude including blacklist and put on holiday the Bidder/Contractor/Concessionaire/Consultant for any future tenders/contract award process. The imposition and duration of the exclusion will be determined by the severity of the transgression. The severity will be determined by the Principal taking into consideration the full facts and circumstances of each case particularly taking into account the number of transgressions, the position of the transgressors within the

company hierarchy of the Bidder/Contractor/Concessionaire/Consultant and the amount of the damage. The exclusion will be imposed for a maximum of 1 year.

3. A transgression is considered to have occurred if the Principal after due consideration of the available evidence concludes that "On the basis of facts available there are no material doubts".
4. The Bidder/ Contractor/Concessionaire/Consultant will its free consent and without any influence agrees and undertakes to respect and uphold the Principal's absolute rights to resort to and impose such exclusion and further accepts and undertakes not to challenge or question such exclusion on any ground, including the lack of any hearing before the decision to resort to such exclusion is taken. This undertaking is given freely and after obtaining independent legal advice.
5. The decision of the Principal to the effect that a breach of the provisions of this Integrity Pact has been committed by the Bidder/ Contractor/Concessionaire/Consultant shall be final and binding on the Bidder/ Contractor/Concessionaire/Consultant, however, the Bidder/ Contractor/ Concessionaire/ Consultant can approach IEM(s) appointed for the purpose of this Pact.
6. On occurrence of any sanctions/ disqualification etc. arising out from violation of integrity pact, Bidder/ Contractor/Concessionaire/Consultant shall not be entitled for any compensation on this account.
7. Subject to full satisfaction of the Principal, the exclusion of the Bidder/Contractor/Concessionaire/Consultant could be revoked by the Principal if the Bidder/ Contractor/Concessionaire/Consultant can prove that he has restored/recouped the damage caused by him and has installed a suitable corruption prevention system in his organization.

Article – 4: Compensation for Damages

1. If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Arcticle-3, the Principal shall be entitled to forfeit the Earnest Money Deposit/ Bid Security or demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security apart from any other legal right that may have accrued to the Principal.
2. In addition to above, the Principal shall be entitled to take recourse to the relevant provisions of the contract related to Termination of Contract due to Contractor/Concessionaire/Consultant's Default. In such case, the Principal shall be entitled to forfeit the Performance Bank Guarantee of the Contractor/ Concessionaire/ Consultant and/or demand and recover liquidated and all damages as per the provisions of the contact/Concession agreement against Termination.

Article – 5: Previous Transgression

1. The Bidder declares that no previous transgression occurred in the last 3 years immediately before signing of this integrity pact with any other Company in any country conforming to the anticorruption/Transparency International (TI) approach or with any other Public Sector Enterprise/Undertaking in India or any Government Department in India that could justify his exclusion from the Tender process.
2. If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action for his exclusion can be taken as mentioned under Article-3 above for transgression of Article-2 and shall be liable for compensation for damages as per Article-4 above.

Article – 6: Equal treatment of all Bidders/ Contractors/ Concessionaires/ Consultants/ Subcontractors

1. The Bidder(s)/Contractor(s)/Concessionaire(s)/Consultant(s) undertake(s) to demand from all sub-contractors a commitment in conformity with this integrity Pact, and to submit it to the Principal before contract signing.
2. The Principal will enter into agreements with identical conditions as this one with all Bidders/Contractors/Concessionaire/Consultant and Subcontractors.
3. The Principal will disqualify from the Tender process all Bidders who do not sign this Pact violate its provisions.

Article – 7: Criminal charges against violating Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s)/ Sub-contractor(s)

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

Article – 8: Independent External Monitor (IEM)

1. The Principal appoints competent and credible Independent External Monitor for this Pact after approval from Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the CMD, RailTel.
3. The Bidder/Contractor/Concessionaire/Consultant accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Bidder/ Contractor/ Concessionaire/ Consultant. The Bidder/ Contractor/ Concessionaire/ Consultant will also grant the Monitor, upon his request and

demonstration of a valid interest, unrestricted and unconditional access to his Project documentation. The same is applicable to Subcontractors.

4. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/Contractor(s)/Subcontractors(s) with confidentiality. The Monitor has also signed on 'Non-disclosure of Confidential Information' and of 'Absence of Conflict of Interest'. In case of any conflict of interest arising at a later date, the IEM shall inform CMD, RailTel and recuse himself/herself from that case.
5. The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Bidder/Contractor/ Concessionaire/Consultant. The parties offer to the Monitor the option to participate in such meetings.
6. As soon as the Monitor notices, or believes to notice any transgression as given in Article- 2, he may request the Management of the Principal to take corrective action, or to take relevant action. The monitor can in this regard submit non-*binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
7. The Monitor will submit a written report to the CMD, RailTel within 8-10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.
8. If the Monitor has reported to the CMD, RailTel, a substantiated suspicion of an offence under relevant IPC/PC Act or any other Statutory Acts, and the CMD, RailTel has not, within the reasonable time taken visible action to proceed against such offence or reported it the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
9. The word 'Monitor' would include both singular and plural.

Article – 9: Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor/Consultant 12 months after his Defect Liability Period is over or 12 months after his last payment under the contract whichever is later and for all other unsuccessful Bidders, 6 months after this Contract has been awarded (In case of BOT projects). It expires for the concessionaire 24 months after his concession period is over and for all other unsuccessful Bidders 6 months after this Contract has been awarded. Any violation of the same would entail disqualification of the bidder and exclusion from future dealings.

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

Article – 10: Other Provisions

1. This pact is subject to Indian Law, Place of performance and jurisdiction is the Registered Office of the Principal, i.e. New Delhi.
2. Changes and supplements as well as termination notices need to be made in writing.
3. If the Bidder/Contractor/Concessionaire/Consultant is a partnership or a Joint Venture partner, this pact must be signed by all partners or members.
4. Should one or several provisions of this agreement turn out to be invalid, the reminder of this agreement remains valid, in this case, the parties will strive to come to an agreement to their original intentions.
5. Issue like warranty / Guarantee etc. shall be outside the purview of IEMs.
6. In the event of any contradiction between the Integrity Pact and its Annexure, the clause in Integrity Pact shall prevail.
7. Any dispute/differences arising between the parties with regard to term of this Pact, any action taken by the Principal in accordance with this Pact or interpretation thereof shall not be subject to any Arbitration.
8. The actions stipulated in the integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

In witness whereof he parties have signed and executed this pact at the place and date first done mentioned in the presence of following witnesses:-

(For & On behalf of the (Principal)

(For & On behalf of Bidder/Contractor/ Concessionaire/Consultant)

Place:
Date:

Witness 1:

_____

Witness 2:

Annexure 7: Complete EoI Examination & Nil Deviation Certificate

(To be submitted by Bidder)

To
Deputy General Manager/ Marketing
RailTel Corporation of India Ltd
Western Railway Microwave Complex
Senapati Bapat Marg, Near Railway Sports Ground
Mahalaxmi, Mumbai – 400013

Sub: Complete EoI Examination & Nil Deviation Certificate

Ref: EoI Number: _____ Dated: _____

Dear Sir,

We <Bidder Name> having completely examined the referred EoI, its corrigendum and any other documents/its addendums/corrigendum referred in this EoI, conclude that we have understood the Terms & Conditions of the EoI and its subsequent addendums & corrigendum (if any) and any other documents/its addendums/corrigendum referred in this EoI. We declare that we have sought all clarifications for the same from RailTel or its end customer for anything contained in this EoI & any other documents/its addendums/ corrigendum referred in this EoI and have been satisfied with the clarifications to the fullest extent and there are no terms, clauses, conditions, etc which are ambiguous.

We also declare that there is no deviation from adhering to anything that is contained in this EoI and any other documents/its addendums/corrigendum referred in this EoI and that any deviation later raised by us shall lead to forfeiture of the Bid/Contract at complete discretion of RailTel.

Signature of Authorized Signatory (with official seal)
Name :
Designation :
Address :
Telephone and Fax :
E-mail address :

Annexure 8: Back to Back Compliance Certificate

(To be submitted by Bidder)

To
Deputy General Manager/ Marketing
RailTel Corporation of India Ltd
Western Railway Microwave Complex
Senapati Bapat Marg, Near Railway Sports Ground
Mahalaxmi, Mumbai – 400013

Sub: Complete back to back Compliance Certificate

Ref: 1) EoI Number: _____ Dated: _____
2) Tender Reference No: CGMIT/RDSS/SDWAN/23-24/014 dated 03-May-2023 and all of its addendums/ corrigendums & published documents

Dear Sir,

Considering reference 1 & 2 we would like to declare that we have read and understood the EoI, its corrigendum and any other documents/its addendums/corrigendum referred in this EoI thoroughly. We would like to give you our back to back compliance for all the tender terms and conditions, clauses, timelines, deliverables and anything explicitly mentioned in the EoI, its corrigendum and any other documents/its addendums/corrigendum referred in this EoI.

Signature of Authorized Signatory (with official seal)
Name :
Designation :
Address :
Telephone and Fax :
E-mail address :

Annexure 9: Performance Bank Guarantee Format

(For a sum of x% of the value of the contract as per RailTel's end customer RFP/tender)
(Stamp Duty and final draft to be confirmed by RailTel in co-ordination with RailTel's Legal Department)

Ref. No. :
Date :
Bank Guarantee No. :

To
<Insert complete postal address>

THIS INDENTURE made this <current date> day of <current Month> 2023, BETWEEN THE <Bank Name>, a Company incorporated and registered under the Indian companies act, 1913 and deemed to exist within the companies Act 1956, and governed by the Banking Regulation Act, 1949 and having its registered office at <Address>, and its corporate office at <Address>, India and having one of its Branch Office at <Mumbai Branch Office> (hereinafter referred to as "the Bank" which expression shall be deemed to includes its successors and assigns) of the first part and
<Bidders Company Name> a company incorporated under the Indian Companies Act 1956 having its Registered Office at <Address>, Corporate Office at <Address> and its Regional Office at <Mumbai Office Address> (hereinafter referred to as 'the Contractor/s') of the second part and
RailTel Corporation of India Ltd (hereinafter referred to as 'RailTel') of the third part WHEREAS the Contractor/s have submitted to RailTel EoI/Quotation for the execution of Procurement, Installation, Commissioning and Management of SDWAN for MSEDCL Field Offices up to Subdivision level vide <EoI No> Dated <Date of EoI> and the terms of such EoI/Tender/Quotation/contract require that the Contractor/s shall deposit with RailTel as the security a sum of Rs. <Amount>/- (in figures and words<in words> only Including all Taxes and contingencies and any other costs mentioned as per LOI and RailTel Terms)AND WHEREAS if and when any such EoI/Tender/Quotation is accepted by RailTel the contract to be entered into in furtherance thereof by the Contractor/s will provide that such deposit shall remain with and be appropriated by RailTel towards the security deposit to be taken under the contract and be redeemable by the Contractors/ if they shall duly and faithfully carry out the terms and provision of such contract and shall duly satisfy all claims properly chargeable against them there under AND WHEREAS the Contractor/s are constituents of the Bank and in order to facilitate the keeping of the accounts of the Contractor/s, the Bank with the consent and concurrence of the Contractor/s has requested RailTel to accept the Guarantee of the Bank hereinafter contained, in place of the Contractor/s depositing with RailTel the said sum as security as aforesaid AND

WHERE AS accordingly <Bank Name>has agreed to accept claim from RailTel upon demand in writing, whenever required by him, from time to time upto <Date (contract period + 3 months)> so to do, a sum not exceeding in the whole Rs. <Amount>/- (in figures and words <in words> only incl of Tax) under the terms of the said EoI/Tender/Quotation and/ or the Contract. The Bank Guarantee is valid up to<Date (contract period + 3 months)>.

Notwithstanding anything what has been stated above, <Bank Name> liability under the above guarantee is restricted to Rs. <Amount>/- (in figures and words <in words>only incl of Tax) and guarantee shall remain in force up to <Date (contract period + 3 months)> unless the demand or claim under this guarantee is made on us and we receive in writing on or before <Date (contract period + 3 months)> all your rights under the above guarantee shall be forfeited and we shall be released from all liabilities under the guarantee thereafter whether or not the original bank guarantee is returned to us.

In witness whereof the Bank, through its authorized Officer, has set its hand and stamp on this …… day of 2022 at ……

For <Bank Name>

Authorized Signatories

EMP No._____

For<Company Name>

Authorized Signatories

EMP No._____

Request for Proposal for Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO

Ref No.: 05/CIDCO/SD/SM/2023-24

Date: October 2023

Tender Processing Fee: ₹ 5,900/- (Non-Refundable) (INR Five Thousand Nine Hundred only including GST)

Systems Manager, Systems Department

First floor, CIDCO Bhavan,

CBD Belapur, Navi Mumbai-400614

Contact number: 022-67918699

Email: sm.tender@cidcoindia.com

Table of Contents

(This page is intentionally left blank)

1. Disclaimer

- City and Industrial Development Corporation of Maharashtra Limited ("CIDCO") has taken adequate care in the preparation of the Request for Proposal (RFP Document). Nevertheless, the Bidder should satisfy itself that the RFP Document is complete in all respects. Intimation of any discrepancy shall be given to this office immediately. If no intimation is received by this office, from any Bidder within five days from the date of issue of this document, it shall be considered that the issued document, which has been received by the Bidder, is complete in all respects.
- Neither CIDCO, nor its employees, consultants, advisors accept any liability or responsibility for the accuracy or completeness of, nor make any representation or warranty - express or implied, with respect to the information contained in the RFP Document, or on which the RFP Document is based, or any other information or representations supplied or made in connection with the Selection Process. Neither CIDCO nor its employees or consultants will have any liability to any Bidder or any other person under any law, statute, rules or regulations or otherwise for any loss, expense or damage which may arise from or be incurred or suffered in connection with any information contained in this RFP Document, any matter deemed to form part of this RFP Document, the award of the Project, the information and any other information supplied by or on behalf of CIDCO or their employees or any consultants or otherwise arising in any way from the Selection Process for the Project.

- The RFP Document does not address concerns relating to diverse investment objectives, financial situation, and particular needs of each party. The RFP Document is not intended to provide the basis for any investment decision and each Bidder must make its / their own independent assessment in respect of various aspects of the techno-economic feasibilities of the Project. No person has been authorized by CIDCO to give any information or to make any representation not contained in the RFP Document.
- Nothing in the RFP Document is, or should be relied on, as a promise or representation as to the future. In furnishing the RFP Document, neither CIDCO, nor its employees, advisors undertake to provide the recipient with access to any additional information or to update the RFP Document or to correct any perceived inaccuracies therein.
- CIDCO or its authorized officers / representatives / advisors reserve the right, without prior notice, to change the procedure for the selection of the Successful bidder or terminate discussions and the delivery of information at any time before the signing of any agreement for the Project, without assigning reasons thereof.
- CIDCO reserves the right to reject any or all of the Bids submitted in response to the RFP Document at any stage without assigning any reasons whatsoever. And CIDCO also reserves the right to change any or all of the provisions of the RFP Document. Such changes will be intimated to all the Bidders.
- Upon the receipt of this RFP Document the Bidder acknowledges the Terms and Conditions of this RFP Document. CIDCO further reserves the right to change, modify, add to, or alter the Selection Process including of additional Evaluation Criteria. Any change in the Selection Process shall be intimated to all Bidders.

2. Tender Notice Published in News Paper

THE INDIAN EXPRESS, TUESDAY, OCTOBER 31, 2023

CIDCO
WE MAKE CITIES

NOTICE INVITING BID

Request for proposal for Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO

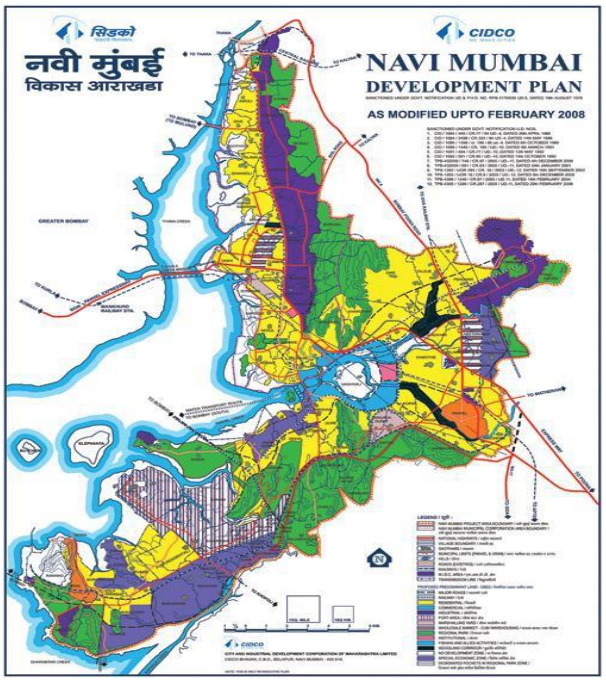
CIDCO through the process of e-Tendering invites **"ONLINE"** Bid from reputed service provider, which shall provide services for "Request for Proposal for Selection of a Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO".

1. Name of Work: Request for proposal for Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO
2. C. A. No.: 05/CIDCO/SD/SM/2023-24
3. Tender Fee: ₹5,900/- (INR Five Thousand Nine Hundred only including GST) (Non-Refundable) for the Tender Fees to be paid through online only. **4. E.M.D. :** Online Payment of ₹4,00,000/- (INR Four Lakhs only) to be paid via online Payment Gateway mode. The information of E-Payment Gateway available on E-Tendering Website https://mahatenders.gov.in **5. Selection Process:** Quality and Cost based selection (QCBS) **GST) 6. Contract Period:** 3 Years or 36 Months

Bid Document along with Bidding programme will be available on the website **https://mahatenders.gov.in**

3. Introduction

- **About CIDCO**



City and Industrial Development Corporation of Maharashtra Ltd. (CIDCO) is a company wholly owned by the Govt. Of Maharashtra and was incorporated on 17th March 1970, with the specific aim of creating a new planned, self-sufficient and sustainable city on the mainland across Thane creek adjoining Mumbai.

CIDCO is designated Special Planning Authority by Government of Maharashtra for new towns to fulfill objectives like reduction of population overcrowding in core cities like Mumbai, Absorption of emigrants and preventing the emigration of present population by providing better conditions and new opportunities,Setting the industrial pace of the State with the help of balanced urban development etc.

Navi Mumbai is known extensively for its judicious planning, earning the city a reputation of being a Super City and one of the largest planned cities in Maharashtra with even distribution of residential areas, job centers, wholesale markets, non-polluting industry and population density.

Infrastructural development, with regards to the Navi Mumbai International Airport, CIDCO Exhibition Centre, SEZ, and Navi Mumbai Metro will help business and companies from around the country and from international quarters enter the versatile market of Navi Mumbai. Projects of international importance are providing the city with ample opportunities in regards with trade and commerce while simultaneously carving the city into a Global Hub. CIDCO, currently, is in the process of improving efficiency and effectiveness in day-to-day operations by implementing state-of-the-art technologies and best practices. This initiative will cover the aspects of urban planning, development and administration in alignment with existing departmental processes and goals while ensuring a cohesive workflow between departments and collaboration amongst various stakeholders within and outside the organization.

- **Background**

The CIDCO official website will act as an integrated platform for all the official information and communication regarding various initiatives undertaken by CIDCO, online services and payment platforms, new schemes initiated by CIDCO, updated notices, news and events. The selected bidder will be responsible for the website's design, development, implementation and maintenance. The proposed website will be hosted through a cloud infrastructure services which is expected to be provided and maintained by selected bidder. The selected bidder shall be required to configure, tune, manage and maintain the production, staging, testing or any such environments hosted on the cloud infrastructure for hosting and maintaining the CIDCO website and related services.

4 Invitation for Proposal

- CIDCO hereby invites Proposals from reputed, competent, and professional service providers, who meet the minimum eligibility criteria as specified in this bidding document.
- The complete bidding document shall be published on https://mahatenders.gov.in/ for the purpose of downloading. The downloaded bidding document shall be considered valid for participation in the electronic bidding process (e-Procurement/ e-Tendering) subject to the submission of required tender/ bidding document fee and EMD online, failing which the bid will be summarily rejected.
- Bidder is advised to study this tender document carefully before submitting their proposals in response to the tender Notice. Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions, and implications.

4.1 Notice Inviting Bid & Bidding Schedule

Sr. No.	Description	Details
1.	Name of Work	Request for proposal for Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO
2.	C.A.No.	To be confirmed
3.	Tender Fee	₹ 5,900/- (INR Five Thousand Nine Hundred only including GST) (Non-Refundable) for the Tender Fees to be paid through online only.
4.	EMD	Online Payment of ₹ 4,00,000/- (INR Four Lakhs only) to be paid via online Payment Gateway mode. The information of E-Payment Gateway available on E-Tendering Website https://mahatenders.gov.in
5	Selection Process	Quality and Cost based selection (QCBS)
6	Performance Bank Guarantee	Successful bidder shall have to pay 3% of total project value as bank guarantee in format as per **Annexure 9.13**
7	Contract Period	3 Years or 36 Months

CIDCO through the process of e-Tendering invites "Online" Bid from reputed service provider, which shall provide services for "Request for Proposal for Selection of a Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO ".

4.2 Bid Schedule

Sr. No.	Critical Dates	(DD.MM.YYYY / Hrs. Mins.)
•	Publishing Date	31.10.2023/17.00 Hrs.
•	Document Download / Sale Start Date	31.10.2023/17.01 Hrs.
•	Last date and time for sending Pre-bid queries	10.11.2023/17.01 Hrs.
•	E-mail id for sending pre-bid queries	sm.dc@cidcoindia.com
•	Document Sale End Date	20.11.2023/17.00 Hrs.
•	Bid Submission Start Date	31.10.2023/17.01 Hrs.
•	Bid Submission End Date	20.11.2023/17.00 Hrs.
•	Bid Opening Date	21.11.2023/15.00 Hrs.

HIMANSHU SHEKHAR

Digitally signed by HIMANSHU SHEKHAR
Date: 2023.10.31 16:24:28 +05'30'

5 Scope of Work

5.1 Redesign and Revamping of Website

The CIDCO website will provide a secure unified access point in the form of a web-based user interface and will be redesigned to publish official information about CIDCO and integrate with other CIDCO's online service platforms. The website should follow GIGW guidelines. This website shall be a source of all information, forms, and payments of different services, etc. for customers and shall act as and operate the required functions.

5.1.1. General Requirement for Website

5.1.1.1. Website architecture

- The website needs to be redesigned with loosely coupled components making it extensible to provision addition of new webpages, online service platforms etc. retaining the existing architecture.
- The website must be developed with the latest version of database management.
- The user interfaces of the system should comply with latest Standard ISO. Latest ISO shall be the standard for guidance on ICT accessibility.
- User Interface (UI) for Website shall be based on responsive design. The application can be accessed over devices of various form factors like desktops, laptops, tablets and mobile.
- Navigation should be designed to help users understand where they are, where they have been and where they can go next. General guidance on achieving self-descriptiveness is given in latest Standard ISO.
- Each presentation segment (page or window) should provide the user with a clear and sufficient indication of where he or she is in the navigation structure and of the current segment position with respect to the overall structure with minimum navigation efforts.
- The system should use HTTPS as the communication protocol.
- The system should run on all the leading browsers (Internet Explorer, Chrome, Firefox, Safari, Opera, Microsoft Edge)
- The system should be designed in manner that operational data is not lost in case of any failure of equipment or communication network.

5.1.1.2. Addition of new application or online services

- The website services should be deployed to have a potential for re-use in launching future services or introducing new application/services, without disturbing the existing architecture.
- The services should also have a potential of having multi-channel access/ integration, as the data returned by the components, would be in XML/OpenXML/XINS /SOAP/JSON/WSDL format.

5.1.1.3. Website language and other integration

- The website must support bilingual versions in English and Marathi. In addition, the website should feature audio enabled content in both the versions (English and Marathi) to aid physically impaired users. The Marathi language implementation needs to be based on Unicode standards.

- The Marathi, English and audio content required for the website will be the service provider's responsibility.
- Currently integration with social media is not part of scope but may be a future requirement. Solution must be capable of integrating with various social media platforms/tools.

5.1.1.4. Content Management (CM)

- The website is the official information & service delivery interface for CIDCO to all the stakeholders and the extreme care shall be taken while designing the website layout, coloring scheme, taxonomy etc.
- One of the key requirements for the website is the content management, which would be the service provider's responsibility to ensure that the content, form and services delivered through website are adhering to the uniform standards.
- To summarize, updation of Static Content shall be the responsibility of the Service Provider (SP) and the Transaction Content shall get dynamically updated via the envisaged System.
- Content management system should be used to add, delete, or modify any pages, pictures, videos, articles etc. on the website.

5.1.1.5. Secure dynamic online self-registration for users

- The website must provide for the ability for users to register themselves in the applicable online service platform. This facility should also give the user the ability to edit details about themselves, such as username and password. If this facility is used to store sensitive information, this should not be redisplayed in its entirety to the user once it has been entered.
- The fields which can be utilised for user registration could include:
    - Name
    - Gender
    - Address
    - Pincode
    - Mobile number
    - Email ID
    - Login username

5.1.1.6. Advanced authentication (including PKI) support.

- The website shall support advanced cloud-based authentication techniques, along with username/password, such as PKI with X.509vs certificates, OATH compliant OTP tokens.

5.1.1.7. "Single Sign-On" capabilities across services

- Single sign-on facility and single user credentials meaning that users can have one user ID and password, or a digital certificate, which they can use for all online public services.

5.1.1.8. Common transaction and routing facility

- Ensuring the reliable delivery of documents and messages. This includes both documents between business and citizens and government, as well as the routing of documents between

government organizations. Secure XML/OpenXML/XINS/SOAP/JSON/WSDL messaging facility enabling secure communication between business, citizens and government organizations.

5.1.1.9. MIS Reporting

- The Website shall provide an interface to the CIDCO to obtain the transaction history, summary and detailed reports on daily transactions, pending applications etc.
- The website shall provide a dash-board view to assess the performance in terms of number of applications received, number of applications processed, pending etc. MIS report generated from the website shall act as a decision support system for the senior officials of the CIDCO.

5.1.1.10. Integration of e-forms with online service applications

CIDCO website hosts various online service application which require user registration via e-forms. The selected bidder must ensure that:

- The size of the e-forms created for delivering the services through website shall be kept to the minimum to suit bandwidth typical to dial-up Internet connections.
- The form filling should be easy, user friendly and have a validation check mechanism to avoid common form filling errors (such as, ensuring all mandatory fields are entered, selecting options by checking boxes where applicable, number entry etc.).
- The website shall provide Easy-to-use step-by-step guidance in form of manual or video to fill the e-Forms.
- The e-Forms, as required for the services, must support Digital Certificate based signatures issued by the authorized CAs. e-Forms may have the need to be signed digitally by the users, depending on the service.
- Website shall provide downloadable and printable pdf formats for all the e-Forms. In addition, upon filling up the details, can obtain the printout of the same. When printed, the e-Form must preserve the appearance as on the screen.
- All the e-forms shall have appropriate field level and form level business validations built into it to ensure that scope for incomplete/ inaccurate information is eliminated, and the information is captured for all the mandatory fields.
- The e-Forms shall be of the format XML/OpenXML/XINS/SOAP/JSON/WSDL or an equivalent format (that meets the all the requirements as described)
- The e-Forms must carry a version identifier and System must ensure use of current version of the form by the users.
- The e-Forms must be supported for use by the stakeholders on all widely used operating systems such as variations / versions of Windows/ Unix/ Linux or any open-source environment, etc., preserving the functionality, look and feel of the form.
- The e-Forms must support attachment of multiple documents. Such attachments must be embedded in the e-Form so that they can be copied/ transported/ uploaded/ downloaded seamlessly together.

- The e-Forms must have facility to allow authorized employees add notes / notations / comments. The facility should allow saving of such notes separately from the e-Form itself. Display of the original e-Form with data should be possible with or without the notes (as per the access privileges applicable).
- Applicants should be able to track the status of their applications.
- On submission of e-form, website should provide acknowledgement with date & time stamp through SMS and e-mail.
- Website should have facility of uploading any attachments in form of PDF, JPEG etc. It should support to customize upload size of an attachment.

5.1.2. Specific Requirements for the Website

Online Service platforms	Requirements
User Login Services 1. COPAS 2. NIAMS 3. Online Grievances Service 4. CIDCO Samwaad 5. Estate Services 6. Mangrove Complaints 7. RTI online Non-User login Services 1. Tenders 2. Citizen Charter 3. Booking-Exhibition, Golf, Urban Haat 4. Development Permission 5. Engineering Services 6. Social Services Schemes 7. 12.5%Land Scheme 8. Vendor Registration	• Should enforce secure login as per the Login process where the government official/staff will have to authenticate his/her Username and Password to access the application and perform the respective functions. Login process for citizen will be finalized during design phase. • Services which do not require logins should be availed without restrictions. • On successful login, system should display a user specific page of application. • Should store all authentication credentials of users in an encrypted format should suspend the user in case of a specified number of unsuccessful attempts to logon to the system and these suspended user IDs should only be reactivated by system. • Should have an audit log capable of recording, displaying and reporting all activity occurring on the portal. • Should time-out after a stipulated period of idle time • Should provide for online help, general information and instructions. • Should not allow any user to upload information beyond their authorized sections. • Should display an appropriate message if the system is unable to process the details due to any reason like connectivity issues, maintenance issues, etc. and provide contact details of the system administrator and alternate link (if available)

	• Should be an online service rather than a static documentation form. • Should enable user registration functionality in the first login attempt and subsequently enable access to the portal from user login functionality. • Should provide easy to use step by step guidance to fill the e-forms. • The e-Forms, as required for the services, must support Digital Certificate based signatures as they need to be signed digitally by the users. • Should have the provision for printable formats for all the e-Forms. • All the e-forms shall have appropriate field level and form level business validations built into it. • Should have a provision to upload the required documents in a relevant format and size on the online portal. • Should display an appropriate error message if the portal is unable to process the details due to any reason like connectivity issues, maintenance issues, etc.

5.1.3. Integration with Online Service Platforms

5.1.3.1. Online payment Services platform

Online payment service platform	Requirements
1. Service Charges 2. Water Charges 3. Marketing plot payment 4. Marketing I & II payment 5. Marketing housing and shop payment 6. Station complex service charge payment 7. NIAMS payment 8. Estate. Misc. receipt payment 9. Copas BP/TP 10. Challan payment-misc. water charges 11. Swapnapurti Payment	• Should provide for and allow financial transaction functions. • Should check for all details of the service before initiating the payment and can submit the application for review before finally submitting the form. • Should enable payment option only when all the fields of service request are filled. • Should highlight & return fields have inconsistencies / error for rectification. • Provision to retain and retrieve information of service request form and all payment records in a database (beside the inconsistencies) • Should return after successful checking of fields with prompt of confirmation to open payment page. • Should open a new page for recording payment details against the service request. • Should allow payment to be registered on service application request against: • Payment against the service • Payment against the dues / payments as defined under service charter of the specific • Should record and maintain all details of payment against a unique service application number. • Should support online payment, including the following fields: • Facilitate payment against dues & recoveries online through a payment gateway (interfaced with a bank) • Supplier may be required to integrate with other payment options as & when required. • Prompt the user to make payment of late fee in case the last date of payment is passed. • Facilitate automatic updation of the information on the applicant record, upon realization of the submitted money. • Payment made should be credited to the proper head of account as per the rules and directives of CIDCO.

	• The system should allow transaction through approved financial instruments such as Credit Cards, Debit Cards and Online Banking • The payment function should be against specific invoice / bills for the given services. • Should ask for the confirmation from user before initiating payment's function. • Should allow for user re-verification before initiating payment function through transaction unique ID allocated to the user. • Should provide for confirmation of transaction to the user and printable version of the payment receipt against the payment. • Should not allow for initiation of payment in case of non-availability of records of invoice / bills. • against which payment function is initiated. System should be able to provide information for such transactions. • Should follow predefined payment rules and regulation as defined from time to time by the application. The same should be updated in the application. • Should maintain all information and records of user transaction tagged to the user account and also provide for viewing of such information as and when required by the user. • Should be able to send emails on user account with respect to payments processing. • Integrated payment gateway should be NPCI or RBI approved.

5.1.4. Security Compliance

The bidder shall appoint a CERT-In empanelled agency who shall be responsible for conducting performance and Security Audit of the website. The CERT-IN empanelled agency appointed by the bidder shall conduct audit before Go-Live and in case of any major change or annually whichever is earlier. The cost of audit and the cost of rectification of non-compliances shall be borne by the Service Provider. The audit shall be performed at least on the below mentioned aspects.

- WCAG
- GIGW
- Performance Testing
- Application Security Audit
- Penetration Testing
- Vulnerability Testing

- Database Server Controls

The illustrative deliverables for this activity are mentioned below:

- First Round Audit Report (by Auditor)
- Rectified solution and submission of next round of audit (by Service provider)
- Next Round Audit Report (by Auditor)
- If required, rectified solution and submission of next round of audit (by Service provider)
- Compliance Confirmation by the Auditor (by the Auditor)

All the above-mentioned activities should get completed before the commencement of go-live. The key activities that need to be performed before Go- live of the solution are as follows:

- Business readiness check before handing over to user.
- Exit Management and Knowledge Transfer Plan
- Mobilization of manpower for hand holding support and maintenance.
- Data Migration to solution
- Approval from client

Note: CIDCO has defined all the possible security standards to be followed by the bidder. If any standard is missed, then service provider should adhere to all such norms.

5.1.5. Website upgrade and version control

All planned changes to application systems shall be coordinated within established Change Control processes to ensure that:

- Detailed impact analysis
- Appropriate communication on change required has taken place.
- Proper approvals have been received.
- Schedules have been adjusted to minimize impact on the production environment.
- All associated documentations are updated post stabilization of the change.
- Version control maintained for software changes.

The Service provider shall define the Website Change Management & Version control process and obtain approval for the same from CIDCO. For any changes to the software, Service provider must prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. Service provider is required to obtain approval from CIDCO for all the proposed changes before implementation of the same into production environment and such documentation is subject to review at the end of each quarter of operations & maintenance support. Service provider should be able to maintain version control of the website. There should also be maker-checker system for any changes being done in website or processes which are part of website. No change shall be made in the production environment without approval from CIDCO authority.

5.1.6. Non-Functional Requirements

- Making user interfaces robust: User interfaces should be designed to be as robust as possible in the face of changing technology. This encompasses being able to present content containing newer technologies by older user agents as well as designing content to be usable with future technologies.
- Acceptable opening / download times: Application pages should be designed and implemented so that there are acceptable opening times and download times for the expected range of technical contexts of use (e.g., bandwidth between the application and the user). This is particularly important for frequently accessed pages or pages that are important for user navigation and exploration, such as the home page.
- Minimizing user errors: Potential user errors as well as the effort needed to recover from errors should be minimized.
- To monitor website uptime and webpage loading time, a System and Network Monitoring tool should be deployed by the bidder.
- An incident management tool must be deployed to create, resolve and manage incident requests.
- Providing clear error messages: The content of error messages shown on the pages or special error pages should clearly state the reason why the error occurred and, if possible, actions the user can take to resolve the error. Users expect error messages to be in the same language as the user interface.
- Using appropriate formats, units of measurement or currency: When designing user interfaces for use by diverse groups, input and output of information elements such as currency, units of measurement, temperatures, date and time, phone numbers, address or postal codes should be designed so that they are usable.
- Making text resizable by the user: Text should be able to be resized by the user, using functions provided by the user agent or other appropriate means i.e., follow ISO standards.
- Text quality: The quality of textual content with respect to spelling and grammar should be sufficient so as not to impede readability.
- Writing style: The reading and understanding of the textual content on the screen should be supported by suitable means, including the use of short sentences, the division of the text into shorter chunks or the presentation of content items in the form of bullet points.
- Fast skimming of text should be supported by the provision of clear links, bulleted lists, highlighted keywords, logical headings, and short phrases and sentences.
- Text presented on the pages should be readable considering the expected display characteristics and spatial arrangement. Latest ISO Standard be consulted for screen text legibility requirements.
- Distinguishable within-page links: Within-page links should be clearly distinguishable from other links that lead to a different page. EX. Within- page links are shown with dashed rather than solid underlines.
- Avoiding link overload: Text pages containing large proportions of links should be formatted so that the presence of links does not impede the readability of the text.
- Using descriptive link labels: The target or purpose of a link should be directly indicated by its label, avoiding generic labels such as "click here" except where the purpose of the link is clear from its context on the page, or the labels have commonly understood semantics in the particular application domain. Using Appropriate terminology specific to the user's tasks and information needs is important for making the content easy to understand.
- Links that open new browser windows or pop-up windows should be clearly marked.

- Distinguishing navigation links from controls: Navigation links should be clearly distinguishable from controls activating some action.
- Use of —white space": —White space" on a page should be used in such a way that it does not impair the visual skimming of the page. While white space is an important means of visually organizing the different content elements on a page, if the distance between the blocks of information displayed. becomes too large, rapid skimming of the page can be impeded.
- Selecting appropriate page lengths. The length of a page should be selected so as to support the primary purpose and use of the page. Short pages are generally more appropriate for homepages, navigation pages, or overview pages that need to be read quickly. Longer pages can be more appropriate when users want to read the content without interruptions or when the page needs to match a paper counterpart.
- Placing title information consistently: Page titles should be placed in a consistent location on the different pages.
- Observing principles of human perception When designing application pages, the general principles of human perception should be considered. The Latest International Standards should be followed.
- Providing a site map: A separate navigation overview such as a site map should be provided for application showing the structure of the site in an overview form.
- The system should be designed to have satisfactory performance even in offices connected on low bandwidth.
- All error messages produced by the System must be meaningful, so that they can be appropriately acted upon by the users who are likely to see them. Ideally, each error message will be accompanied by explanatory text and an indication of the action(s) which the user can take in response to the error.
- The Interface should be simple, soothing to eye, attractive, uncluttered.
- The System must employ a single set of user interface rules, or a small number of sets to provide a familiar and common look and feel for the application.
- The System must be able to display several entities simultaneously.
- The System must provide End User and Administrator functions which are easy to use and intuitive throughout.
- Frequently executed System transactions must be designed so that they can be completed with a small number of interactions (e.g., mouse clicks).

5.2. Migration from SDC to cloud

5.2.1. Migration Service

CIDCO is currently hosting its website in state data center. As per the new directives from DIT, it is now required to avail new Cloud services or renew existing Cloud services. All online applications of CIDCO will be hosted on the availed cloud services. CIDCO's website will also be hosted on the availed cloud services among other applications. SI has to choose the Cloud Service Provider (CSP). The CSP shall be MeITY empaneled as per Ministry of Electronics and Information Technology (MeITY) guidelines as on bid submission date offering both DC & DR and should follow all technical guidelines as mentioned by MeITY.

5.2.1.1. Pre-requisites

- Following tasks shall be carried out to determine the current inventory, assess the current environment to determine which workloads and applications are critical and because of which there may be a loss to CIDCO:

- Analysis to identify the IT users and stakeholders that would be impacted by cloud migration.
- Identify the business processes and governance processes that are associated with current inventory (both applications & infrastructure).
- Formulated a baseline of CIDCO's technical environment including inventory of both infrastructure and applications, to include development/testing environments.
- Successful bidder shall provide Application Management Services during migration period.
- Successful bidder would be required to understand the complete Application landscape so as to provide Application management.
- All the required support for application to ensure its smooth running, data consistency, performance will be responsibility of successful bidder.
- Understanding of the implications of moving individual applications or groups of applications to the cloud.
- Decomposition of applications & identification of common functions and services that can potentially be migrated to the cloud, and identification of potential shared services. Comprehensive analysis and understanding of the current environment, that incorporates considerations for security such as data sensitivity, legal or other regulatory issues, disaster recovery and analysis of which on premise technical resources / applications are best suited for the cloud.

5.2.1.2. Migration Planning

- Comprehensive planning for migration of the application suite and data to the cloud including developing the migration roadmap identifying the constraints and inhibitors to cloud migration. The migration plan should detail out:
  - The configuration proposed to fulfil day-1 requirements with the explicit understanding that during the duration of the contract these nominal profile requirements will change.
  - Migration Tools, software, applications, scripts, and associated licenses has to be planned and documented.
  - Procedures and documentation to be developed for migration of applications and data & content including redevelopment/additional development that may be required.
  - Plans for co-existence of non-cloud and cloud architectures during and after migration.
  - Communication, change management, and training needs.
  - Cloud governance for post-implementation
  - Test Plans for verifying successful migration.
  - Detailed Risk Management Plan that will identify potential risks, set out possible mitigation approaches, and identifies specific tasks the successful bidder will undertake to help avoid identified risks connected with the Migration.

5.2.1.3. Migration

- Changes to the applications based on:
  - Complete architectural understanding of the existing applications and processes necessary for successful migration of the applications and data as well as continued operation and maintenance of the services.
  - Analysis of the interdependencies such as application dependencies and affinities to servers, server configuration etc.
  - Dependencies between applications and data.
  - Provision the necessary compute & storage infrastructure on the cloud including the underlying software licenses to host the Application Suite that meet or exceed the day-1 minimum capacity.

- Setup of Development, Quality, Production and Disaster Recovery Environments by provisioning the necessary compute & storage infrastructure on the cloud along with the underlying software licenses to host the Application Suite.
- Configuring external connections to the hosted infrastructure required to upload database backups and virtual machine (VM) images to the hosting environment.
- Migration of the Application Suite from the existing infrastructure to the cloud infrastructure. The migration (supported by service provider) shall also include the migration of underlying data & files from the current database(s) / storage into the database(s) / storage on the cloud.
- To enable easy migration to cloud, CIDCO may consider up-gradation of OS & DB to latest version available in market.
- Deployment of the new Applications on the cloud environment as per the to be architecture.
- Configure, manage, deploy, and scale the system on environments setup on cloud.

5.2.1.4. Managing and Monitoring of Migration

- Manage (including project managing), coordinating and planning all aspects of migration.
- Proactively identify, monitor, and manage any significant risks or issues in relation to migration.
- Provide regular progress reports to CIDCO.
- A listing of all Migration Deliverables and Milestones, including acceptance status, the estimated time to completion, days overdue, planned completion date, and actual completion date and comments, as well as a report identifying the status of all Milestones (for example: red, amber, green).
- A listing of all unresolved issues related to the execution of the Migration Plan, along with due dates, priority, responsible party, and an assessment of the potential and actual business impact and impact to the Migration Plan. Status of the any risks, including those identified in the Risk Management Plan, as well as the steps being taken to mitigate such risks.
- The successful bidder must prepare a backup plan to address failure in the migration activity. The bidder must implement the backup plan post review and approval by CIDCO. The progress of the backup plan must be provided to CIDCO.

5.2.1.5. Migration Backup plan

- Proactively create a Migration Backup Plan in case of migration failure from state data centre to cloud services for CIDCO's application.
- The Migration backup plan should include a series of steps undertaken to retrace the migration activity to state data centre in case a failure has been encountered.
- The migration backup plan must also include due dates, responsible party and an assessment of potential and actual business impact which should be approved by CIDCO.
- Post the backup migration activity, the hosted applications must function as its original state Any error in the system workflow must be treated as an incident and resolved by the selected bidder as per the defined SLA.

5.3. Cloud Services

The broad project scope includes having a single service provider to provide cloud hosting and managed services for CIDCO. CIDCO intends to procure the Government Community Cloud / Virtual Private Cloud Hosting & Managed Services for the business applications of CIDCO. The shortlisted service provider shall shortlist CSP and provide hosting on the Government Community Cloud Hosting / Virtual Private Cloud & Complete Managed Services, migrate the complete workload from

existing Cloud to newly selected service provider for the period of 3 years, CIDCO reserves the right to extend the services up to 2 further years based on the performance of the bidder.

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 CIDCO.

The broader requirements are expressed in the below –

- Cloud Infrastructure for Application Hosting (DC and DR)
- Migration from existing Cloud infrastructure to the infrastructure of the newly selected service provider
- Cloud Managed Services

5.3.1. General Requirements

CIDCO is looking forward for the delivery of the following broad areas of services under this project:

5.3.1.1 Deployment of solution on Government Community Cloud (GCC) or Virtual private Cloud (VPC)

- The Proposed Smart Governance Solution shall be hosted in Cloud environment, Virtual Private Cloud/ Government Community Cloud Hosting
- Successful Bidder has to choose the Cloud Service Provider (CSP). The CSP shall be MeITY empaneled as per Ministry of Electronics and Information Technology (MeITY) guidelines as on bid submission date offering both DC & DR and should follow all technical guidelines as mentioned by MeITY.
- Successful Bidder has to quote all the required components including but not limited to Compute, Virtual Machines (VMs), software, licenses, cyber security components, storage, etc. in BOQ.
- Successful Bidder shall be completely responsible for the installation, testing and certification of the necessary software licenses required to deploy the Smart Governance system applications at the Cloud Data Centre and at the Disaster Recovery Centre.
- Successful Bidder should ensure that the redundancy requirements are met, infrastructure procured by the successful bidder to have redundancy-built in. Successful Bidder shall also provide descriptive 'Deployment Model, Diagrams (HLD & LLD) and Details' so that redundancy requirements for the common data center infrastructure can be addressed.
- Successful Bidder should ensure that the cloud architecture needs to be scalable to meet future demands and provide sufficient levels of security and interoperability so that CIDCO customers (internal and external) are comfortable having critical infrastructure hosted in a safe environment.
- Successful Bidder should provide complete access for monitoring of infrastructure to CIDCO including but not limited to Virtual Machine, Storage, Backup, Security, Network, Firewall, Load Balancing, Disaster Recovery, Data Replication, Internet Bandwidth/Data Transfer, DDOS, WAF, etc.
- Successful Bidder should provide on-demand full administrative access to CIDCO of infrastructure including but not limited to Application Data, Databases, Virtual Machine, Storage, Backup, Security, Network, Firewall, Load Balancing, Disaster Recovery, Data Replication, Internet Bandwidth/Data Transfer, Software, license, migration, monitoring, etc.
- Successful Bidder will be responsible for providing Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data centre meet the RPO and RTO requirements.

- Successful Bidder should ensure that the RTO shall be less than or equal to 1 hours for all the databases & critical applications and 2 hours for all non-critical applications and RPO should be less than or equal to 15 minutes i.e., the replication cycle should run at maximum 15 minutes for all databases and critical applications and 1 hours for non-critical applications.
- Successful Bidder should ensure that the RPO monitoring, Reporting and Events Analytics for the Disaster recovery solutions is part of the offering. CIDCO reserves the right the reject the Bid technically if reporting and monitoring component is overlooked by the service provider.
- The selected Successful Bidder would be solely responsible for implementation of all tools and software at DR site. All costs including licenses/subscription/support for Software, OS, Replication Tools, etc. if any shall be borne by the selected Successful Bidder
- Successful Bidder to size and provide connectivity for replication between Primary DC and DR Site. Cost of replication and connectivity charges should be part of DR Solution (DRaaS).
- Successful Bidder will be responsible for Automated switchover/ failover facilities (during DC failure & DR Drills) are provided. The switchback mechanism should also be automated. The selected bidder should also provide a tool/ mechanism for CIDCO Cloud DC to trigger DR switchover, for example a "One-Click DR".
- The Successful Bidder should offer dashboard to monitor RPO of each data type.
- Successful Bidder should ensure that the solution should be capable of enabling automatic scale-up and scale-down of services hosted in the Cloud DC-DR on demand or other factors, shall ease infrastructure management, shall be agnostic to the underlying hardware, storage, network, operating system, and hypervisor and shall support open format for virtual machine images.
- Successful Bidder will be responsible for sizing the hardware/compute to support the scalability and performance requirements of the solution. The Successful Bidder shall ensure that the servers and storage are sized adequately, and redundancy is built into the architecture that is required to meet the service levels mentioned in the RFP.
- Successful Bidder should provide all the testing and compliance report and fulfil the FAT requirements, after commissioning and testing of the entire system at CSP Data Centre and DRC.
- Successful Bidder should ensure that all the certifications and reports should be submitted to the CIDCO upon request or as per requirement.
- The entire Network Path for each of the hosted Department applications shall be logically separate from that of other government departments.
- The entire Network path of us shall be administered through a Firewall with secured VLAN zoning.
- Successful bidder shall administer the Firewall policy as per CIDCO's directions. The successful bidder shall also enable CIDCO to administer the firewall policy remotely. successful bidder shall also provide read-only access of the firewall configuration to authorized officials from CIDCO.
- With respect to monitoring tools, if any agent has to be deployed on the VMs or otherwise, the monitoring tools may be shared provided there is logical segregation and controls built-in to ensure that the tools & deployed agents comply to the security policies and ONLY the events, performance threshold alerts and inventory data for the OS, DB, infrastructure and Application is captured & sent by the deployed agents. The monitoring tools and deployed agents (in case of agent-based tools) shall not capture or send Government Department's application and/or user and/or transaction data.
- Security solutions such as UTM, WAF, Anti-Virus, Anti-DDoS etc. shall be deployed for securing CIDCO applications.

- Successful bidder shall offer DR cloud services with their Data Centre location within India only. Successful bidder shall ensure that the CIDCO's data resides within India only.
- The NOC and SOC facility must be within India for the Cloud Environments and the managed services quality should be certified for ISO 20000:1.
- The DR Solution shall be on Active (DC) – Standby (DR) mode.

5.3.1.2 Design of cloud infrastructure

- Successful bidder shall set up and manage the entire cloud solution deployed for CIDCO by Provisioning and Managing Cloud based resources on subscription based / OPEX Model only.
- The proposed solution must support multi-tenant environment.
- The Successful bidder should ensure that the DC & DR site location is within India and the one of the DC is in Maharashtra.
- Successful bidder shall adequately size the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels (cloud services) mentioned in the RFP and the application service levels.
- Successful bidder shall provide a detailed solution document for setting up of the DC & DR. The same shall be approved by the CIDCO- System Manager /project in-charge.
- Subsequently, the successful bidder shall provision the entire infrastructure (compute, storage, network, security, software, bandwidth etc.) required for setting up of the DC & DR site as per the approved solution document.
- Successful bidder shall follow Scope of Work, Policies and Procedures defined by MeITY, GoI. CERT-IN time-to-time.
- Successful bidder shall carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution. There should not be any constraints on the services.
- The successful bidder shall ensure that all peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.
- CIDCO will not be responsible if the successful bidder has not provisioned some components, subcomponents, assemblies, and sub-assemblies as part of Infrastructure Bill of Material and Bill of Quantity.
- The successful bidder will have to provision the same to meet the solution requirements at no additional cost and time implications to CIDCO.
- The Cloud services shall be available on pay as per usage model. The billing shall be done quarterly irrespective of Fixed, On- Demand or mixed model of the Cloud Service Provider.

5.3.1.3 Infrastructure Analysis and Build

- Successful bidder shall provide complete hardware details at DC & DR site including following parameters.
    - CPU Calculation
    - RAM Calculation
    - Disk Calculation
    - Network interface requirement
    - Network throughput requirement
    - Backup requirement
    - Bandwidth Usage

- Successful bidder shall provide direct leased-line connections between CIDCO- DC site and the CIDCO - DR, if required or secured access must be provided to office users.
- Successful bidder shall size the bandwidth requirements for the same and the internet pipeline shall be protected from DDoS attack. It is to be noted that CIDCO mandates for connectivity through the established ISPs.
- Proposed Solution should be compatible with IPv6 and High-level architectural diagram showing different layers of solution like Internet / P2P Connectivity, Network, Security, Compute, Hardware, Storage & Backup layers.
- Proposed solution should have IP schema depicted at high level with NAT to secure the applications directly getting exposed to Internet. Successful bidder should propose to deploy different applications and database in different VLANs with restricting users to directly access database layer and storage layer.
- Successful bidder shall provide Backup solution with different features, like snapshots of VMs, RDBMS backup, incremental and full back up of all data, restoration of data in test environment or as and when required.

5.3.1.4 Dynamic Scaling of Resources

- The initial sizing & provisioning of the underlying infrastructure (including the system software and bandwidth) shall be carried out based on the information provided in the RFP.
- Subsequently, the successful bidder shall scale up (or scale down) the resource requirements (compute, memory, storage, bandwidth etc.) based on the growth in the user compute load / data load / bandwidth load (during peak and non-peak periods / year- on-year increase) to support the scalability and performance requirements of the solution and meet the SLAs. There should not be any constraints on the services.
- There should be sufficient headroom (at an overall level in the compute, network and storage capacity offered) available for near real time provisioning (as per the SLA MeITY) during any unanticipated spikes in the user load.
- The scaling up / scaling down has to be carried out with prior approval by CIDCO.
- The successful bidder shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilizations, expected growth / demand and any other details justifying the request to scale up or scale down.
- For any changes to the underlying cloud infrastructure, software, etc. under the scope of the successful bidder, CIDCO shall get alerts / notifications from the successful bidder, both as advance alerts and post implementation alerts.
- Auto scaling upto 20% of current resources should be non-chargeable.

5.3.1.5 Ownership of Data / VMs/ Software

- CIDCO shall retain ownership of all data & applications hosted on successful bidder's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time (without additional charges).
- CIDCO retains ownership of all virtual machines, templates, clones, and scripts/applications created for CIDCO's application. CIDCO retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time (without additional charges).
- CIDCO retains ownership of loaded software installed on virtual machines and any application or product that is deployed by CIDCO on the Cloud Infrastructure.

5.3.1.6 Compliances

- Successful bidder shall adhere to the standards published (or to be published) by CIDCO or any standards body setup / recognized by Government of India and notified to the successful bidder by CIDCO as a mandatory standard.
- The successful bidder's cloud service offerings shall always remain empaneled / complied with the MeITY guidelines & standards. Successful bidder shall be responsible for the costs associated with implementing, assessing, documenting, and maintaining such Empanelment/Compliances.
- Successful bidder shall always remain adhered to the prevailing guidelines issued by NCIIPC, RBI, CERT-In etc. from time to time.

5.3.1.7 Documentation

- Successful bidder shall create and maintain all the necessary technical documentation, design documents, standard operating procedures, configurations required to continued operations and maintenance of cloud services.
- The documents which hold critical information, process, policies shall have to be approved by CIDCO before release.
- The successful bidder shall develop, maintain, update following documents as per CIDCO's requirements as mandatory documentation compliance:
    - Details of inventory for Compute, Storage, Network, Security elements.
    - Details of the management, monitoring and helpdesk tools
    - The WAN connectivity plan
    - Business Continuity/DR plan
    - Details of manpower deployment at NOC and SOC
    - Escalation matrix.
    - Other details as desired by CIDCO

5.3.1.8 Resource Management

- The successful bidder shall manage the instances of storage, compute instances, and network environments. This includes CIDCO owned & installed operating systems and other system software that are outside of the authorization boundary of the successful bidder.
- The successful bidder shall provide a webpage and associated Uniform Resource Locator (URL) that describes the following:
    - Service Level Agreements (SLAs)
    - Help Desk and Technical Support
    - Resources (Documentation, Articles/Tutorials, etc.)

5.3.1.9 Operation Services

- Successful bidder shall ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.
- Successful bidder shall manage the network, storage, server, and virtualization layers, to include performance of internal technology refresh cycles applicable to meet the SLAs.
- Successful bidder shall ensure monitoring of 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 within the successful bidder's boundary.
- Prepare a comprehensive O&M plan for managing the cloud services and keep it updated.

- Successful bidder shall ensure uptime and utilization of the cloud resources as per SLAs defined in this RFP.
- Successful bidder is required to alert CIDCO when the utilization exceeds 80% and provision additional VMs upon approval from the CIDCO.
- Successful bidder shall manage the cloud infrastructure as per standard ITIL framework.
- Successful bidder shall investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools.
- Successful bidder shall design and implement automated scaling processes.
- Any required version/Software upgrades, patch management etc. at the Cloud Site will be supported by the successful bidder for the entire contract period at no extra cost to CIDCO.
- Successful bidder shall provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.
- Successful bidder shall document and perform patch management appropriate to the scope of their control and/or provide self-service tools to perform patch management. Generate alerts well in advance on the upcoming patches via email and management portal.

5.3.1.10 Self Service Management /Provisioning

- Self Service management / provisioning focuses on capabilities required to assign services to users, allocate resources, and services and the monitoring and management of these resources.
- The successful bidder shall provide Self Service Provisioning Portal / Basic monitoring tool / Dashboard with two factors authentications via the SSL/TLS or SSH or through a web browser to remotely administer their virtual instances having fine-grained role-based access controls.
- It shall enable CIDCO to provision virtual machines, storage, and bandwidth dynamically (or on-demand), on a self-service mode or as requested.
- It shall enable service provisioning via online portal/interface (tools).
- It shall enable service provisioning via Application Programming Interface (API).
- It shall enable secure provisioning, de-provisioning and administering [such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH)]
- It shall Support the terms of service requirement of terminating the service at any time (on-demand).
- It shall make the Management Reports described in this RFP accessible via online interface. These reports shall be available till contract duration after being created.
- The successful bidder shall provide for automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means.
- The Utilization Monitoring tools shall have minimum following features:
    - Real time performance thresholds.
    - Real time performance health checks.
    - Real time performance monitoring & Alerts.
    - Historical Performance monitoring and reporting
    - Capacity utilization statistics for e.g., utilization report of components like RAM, CPU, Storage and network link
    - Cloud resource usage including increase / decrease in resources used during auto-scale.
- The successful bidder shall provide ticketing (Trouble Ticket / issuing reporting / change request etc.) via online portal/ interface (tools).
- Successful bidder shall provide network information of cloud virtual resources.
- Successful bidder shall provision to monitor latency to cloud virtual devices from outside world.

- Successful bidder shall provision to monitor network uptime of each cloud virtual machine.
- Successful bidder shall provision for resource utilization i.e., CPU graphs of each virtual machine.
- Successful bidder shall provision for resource utilization graph i.e., RAM of each virtual machine.
- Successful bidder provision for resource utilization graph i.e., disk of each virtual machine. There shall be graphs of each disk partition and email alerts should be sent if any threshold of disk partition utilization is reached.
- Successful bidder shall provision to monitor the uptime of cloud resources. The report shall be in exportable form.
- Successful bidder shall provision to monitor the load of Linux/Windows servers and set threshold for alerts.
- Successful bidder shall provision to monitor the running processes of Linux/Windows servers. This will help CIDCO to take the snapshot of processes consuming resources.
- Successful bidder shall provision for setting alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.
- Successful bidder shall ensure that there should be audit logs of minimum 6 months for resource utilization to resolve any billing disputes if any.
- Successful bidder shall ensure that audit logs of scalability i.e., horizontal, and vertical is maintained for minimum 6 months so that billing disputes can be addressed.
- Successful bidder shall ensure that log of reaching thresholds used to trigger additional resources in auto provisioning are maintained.
- Successful bidder shall ensure that there are sufficient graphical reports of cloud resource utilization and available capacity.
- Successful bidder shall provide utilization reports for internet bandwidth, load balancers etc.
- Successful bidder shall provide ability of monitoring & management of network link proposed as part of this solution.
- Successful bidder shall provide ability to display monitoring parameters for continuous monitoring bandwidth utilization, latency, packet loss etc.

5.3.1.11 User Administration

- Successful bidder shall Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege principles and ensuring that users have only those permissions necessary to perform their assigned tasks.
- Successful bidder shall facilitate Administration of users, identities, and authorizations, effectively managing the root account, as well as any Identity and Access Management (IAM) users, groups, and roles they associated with the user account.
- Successful bidder shall Implement Multi-Factor Authentication (MFA) for the root / admin account, as well as any privileged Identity and Access Management accounts associated with it for cloud portal.

5.3.1.12 Help Desk

- Successful bidder must provide multiple support options catering to the varying levels of support requirements (e.g., toll free number, ticket, chat, and forum) for CIDCO.
- CIDCO System Manager shall be periodically visiting the data center site on quarterly basis or as and when required. successful bidder shall make convenient & secure provisions for at least

2 CIDCO personnel to access CIDCO cloud infra and meeting with stack holder who all are providing the support service to CIDCO.

- The successful bidder must have Fire-proof workspace. Fireproof workspace should be under 24 x 7 CCTV monitoring.
- If CIDCO asks, then successful bidder should ensure availability of at least one dedicated support person in CIDCO premises for providing the required support.

5.3.2 Cloud Compute Requirements

5.3.2.1 Managed Virtual Machine

5.3.2.1.1 Provisioning of Virtual Machines (VM)

- The Successful Bidder shall do provisioning for required computing resources for hosting of all the required IT applications as listed. Application and DB servers shall be deployed on enterprise class Virtualized environments.
- Virtual Machines shall be required to run the variety of workloads such as compute-intensive workload, memory-intensive workload, general-purpose workload, etc.
- The Successful Bidder shall deploy VMs on Server-Hardware having 1:2 Physical Core to vCPU ratio.
- CPU (Central Processing Unit) shall be provided with a minimum equivalent processor speed of 2-4GHz. CPU launch year should be after year 2015. CPU shall support 64-bit operations.
- The virtual machine shall be capable of running different operating systems (Linux, Windows etc.) with any of their variants/ versions.
- Operating System license to be provided by CSP and bundled with VM at no extra cost.
- Successful bidder shall be able to support major Linux distributions - (Oracle Linux, Red Hat, SUSE, Ubuntu, Centos, and Debian etc.)
- Successful bidder shall offer license portability and support for Microsoft products etc.
  Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, lOPS and network.
- CIDCO retains ownership of all virtual machines, templates, clones, and scripts/applications created for the CIDCO's application.
- Provide facility to configure virtual machine of required vCPU, RAM and Disk.
- Provide facility to use different types of disks like HDD, SAS, SSD based on type.
  of application.
- Service shall allow users to load applications and data securely and remotely onto the virtual machine.
- Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing.
- The successful bidder should offer fine-grained access controls including role-based access control, use of SSL certificates, or authentication with a multi-factor authentication.
- The successful bidder should ensure Installation, Configuration, Commissioning/Decommissioning and Management of the Virtual Machines and provide CIDCO the access to the same via a secured Cloud Management Portal
- In case of suspension of a running VM, the VM shall still be available for reactivation for a reasonable time (30 days) without having to reinstall or reconfigure the VM for CIDCO. In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted, destroyed, and certify the VM and data destruction CIDCO as per stipulations and shall ensure that the data cannot be forensically recovered.
- CIDCO retains the right to request full copies of these virtual machines at any time.

- CIDCO retains ownership of CIDCO loaded software installed on virtual machines and any application or product that is deployed on the Cloud by CIDCO.
- CIDCO should be permitted to bring and upload additional licensed nonoperating system software for operation in cloud as required for the CIDCO solution for use within the Services by installing it directly on a VM.
- VM should support both Horizontal as well as Vertical Scaling

5.3.2.1.2 Administration, Configuration & Training

- Upon deployment of virtual machines, the successful bidder has to assume full administrator access and is responsible for performing additional configuration, security hardening, vulnerability scanning, application installation, troubleshooting, hardening, patch/ upgrades deployment, as and when required.
- Successful bidder shall ensure Preparation / Updation of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening.
- Successful bidder shall ensure Patching of VMs on the next available patch management change window and / or provide self-service tools to patch VMs.
- The successful bidder shall be setting up and configuring servers and applications as per configuration documents/ guidelines provided by CIDCO.
- The successful bidder shall do Installation/ re-installation of the server operating systems and operating system utilities in the VMs.
- Successful bidder shall monitor availability of the servers, successful bidder-supplied operating system & system software, and successful bidder's network.
- successful bidder shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection, and backup functions.
- Successful bidder shall arrange training for CIDCO personnel on proposed cloud platform from OEM with certification.
- Successful bidder shall perform patch management appropriate to the scope of their control and/or provide self-service tools to perform patch management. Any required version/Software, patch management etc. at the Cloud Site will be done by the successful bidder for the entire contract period.
- Updating of application / patch updating will be done by the vendor team of CIDCO.
- Successful bidder shall document all patch management related activities within the successful bidder's scope.

5.3.2.1.3 Internal Storage Requirements of VMs

- The successful bidder shall provide scalable, redundant, dynamic Web-based storage.
- The successful bidder shall provide SSD based storage.
- The successful bidder shall provide options to use different types of disks based on performance requirement of the hosted application stack. Once mounted, the block storage should appear to the virtual machine like any other disk.
- Successful bidder shall enable CIDCO to add either block storage volume or file level storage block to cloud VM from provisioning portal.
- There has to be different disk Space options to allocated for virtual machines and file data as per the requirement of CIDCO.

5.3.2.1.4 Network Interfaces & Segmentation of VMs

- Successful bidder shall ensure that cloud VM network is both IPV4 & IPV6 compatible.
- Successful bidder must ensure that cloud virtual machines are into separate virtual LAN.

- Successful bidder shall provide Private static IP addresses for all the VMs.
- Successful bidder must ensure that all the cloud VMs are zoned in different network segments (VLANs) as per CIDCO requirements.

5.3.2.1.5 Security of VMs

- VMs should be firewall protected.
- VMs should have Host based Security Software.
- The successful bidder shall provide Identity and Access Management for managing access to CIDCO users.
- Hardening & patch management of underlying infrastructure by successful bidder
- Management of the OS processes, antivirus, malware removal software and log files of the VMs
- Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.
- Management of the OS processes and log files including security logs retained in guest VMs.

5.3.2.1.6 Server Load Balancing

- CSP/Bidder should deploy a Load Balancer to distribute the TCP, UDP, HTTP, HTTPs traffic across many computing resources within the same site to increase the responsiveness and availability of applications.
- Cloud service should provide secure, hardened, redundant (hardware or software) based Load balancer services.
- Load Balancer should support both Internet and Intranet traffic.
- The selected CSP shall provide Instance based Load balancing service with web-based interface and below mentioned features including but not limited to.
    - Layer 4/ Layer7 LB with minimum 1Gbps throughput
    - HTTP Caching &Data Compression
    - Application Acceleration & Monitoring
    - Comprehensive application Security
    - TLS/SSL Offload
    - HTTP Compression
    - TCP offload
    - LDAP,AD, RADIUS Authentication, SAML support

5.3.2. Data Handling

- The successful bidder shall strictly maintain isolation of the CIDCO'S data isolated from another client in multi-tenant environment. Provide and implement security mechanisms for handling data at rest and in transit.
- In order to maintain confidentiality of the CIDCO's data, successful bidder shall further ensure with an undertaking that the data cannot be forensically recovered after its deletion. The successful bidder should provide tools and mechanism to CIDCO or its appointed agency for configuring, scheduling, performing, and managing back-ups and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases, and enterprise applications in an encrypted manner as per the defined policy.
- The successful bidder shall manage data recall throughout the data life cycle. successful bidder shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of CIDCO.

- The successful bidder shall provide mechanism to transfer data back in-house either on demand or in case of contract or order termination for any reason. On expiration/ termination of the contract, successful bidder shall handover complete data in the desired format to CIDCO which can be easily accessible and retrievable.

5.3.3. Provisioning of Database Servers and DBA Services

- The successful bidder will be. responsible for administration, configuration management and monitoring of database server, security and databases as per CIDCO's requirement.
- The successful bidder must provide the following options for Databases in their environment.
  - laaS for hosting DB on VMs
  - PaaS for Managed Database as a service for end-to-end DB services
  - PaaS for NoSQL dataset services
- The Managed Database as Service should support all major databases including but not limited to
  - MSSQL
  - MySQL
  - PostgreSQL / Enterprise DB
  - Oracle
- CIDCO reserve right to bring their own database license and use the same on Cloud DC& DR environment. In case, database license is provided by CIDCO, the successful bidder will be still responsible to database administration & management, monitoring, backup and performance tuning.
- The successful bidder should provide tools for monitoring performance of database and provide tools for optimizing query performance and tuning.
- The successful bidder shall be responsible for managing and updating security patches after approval form CIDCO.
- Successful bidder shall provide ability monitor table health and size.
- Successful bidder shall provide ability to display live and waiting session.
- Successful bidder shall provide solution for Monitoring Parameters Buffer Cache Size, Shared Pool Size
- Successful bidder shall provide solution for Monitoring Parameters Redo Log Buffer Size, Fixed Area Size
- Successful bidder shall provide solution for Monitoring Parameters Java Pool size, Free Memory, Total free able PGA, Maximum PGA allocated, Total PGA allocated, Total PGA used, Cache Hit Percentage.

- Successful bidder shall perform following Database support services:
  - Installation, configuration, maintenance of the database (Cluster & Standalone).
  - Regular health check-up of databases.
  - Regular monitoring of CPU & Memory utilization of database server,
  - Alert log monitoring & configuration of the alerts for errors.
  - Space monitoring for database table space, Index fragmentation monitoring and rebuilding.
  - Performance tuning of Databases.
  - Partition creation & management of database objects, Archiving of database objects on need basis.
  - Patching, upgrade & backup activity and restoring the database backup as per defined interval.

- Schedule/review the various backup and alert jobs.
- Setup, maintain and monitor the 'Database replication' and Assess IT infrastructure up-gradation on need basis pertaining to databases.

5.3.4. Storage Provisioning

- Successful bidder shall do provisioning for required storage for hosting of IT applications.
- Successful bidder shall provide scalable, dynamic, and redundancy storage. successful bidder shall offer Block / File Object level storage to use with compute instances in the cloud.
- Successful bidder shall have following storage offerings to address different kind of CIDCO's needs.
- Successful bidder shall provide facility to use different types of disks like SAS, SSD based on type of application. Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads.
- The application and database storage shall be provided on high-speed disks (minimum 5 IOPS/GB) for better performance. Successful bidder shall deliver disks with minimum IOPS per GB for OLTP load. The IOPS for NON OLTP load should be minimum 2 IOPS per GB.
- Successful bidder shall allow minimum block of 1 GB to be provisioned by CIDCO from self-service provisioning portal.
- Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
- Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).

5.3.5. Backup & Restore Service

- Successful bidder shall provide backup solution as mentioned in **Annexure 9.2.8** 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.
- Successful bidder shall cover (not limited to) Backup & Restoration of VM images, Operating System, Applications, Databases and File system etc.
- Successful bidder shall provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing. It shall allow take an existing running instance (or a copy of an instance) and export the instance into CIDCO's approved image format. Entire VM data backup must be available to CIDCO.
- Successful bidder 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 CIDCO.
- Successful bidder shall also perform Administration, tuning, optimization, planning, maintenance, and operations management for backup and restore.
- Successful bidder should propose cloud native solution or use a SaaS based/Third Party Software deployed on VM based backup software.
- The Long-Term Storage should have an option of enforcing WORM (Write Once, Read Many) policy for section of data that requires the same.
- The backup service should support granular recovery of virtual machines, database servers, Active Directory including AD objects, etc.

- CIDCO should be able to recover individual files, complete folders, entire drive or complete system to source machine or any other machine available in network.
- Successful bidder shall restore the requested data with the objective to initiate a minimum of 95 percent of the total number of restore requests per calendar month for data that can be restored from a local copy.
- Successful bidder shall Provide and install additional infrastructure capacity for backup and restore.
- There must be provision if required to shift the backup at CIDCO required location on tape/USB.
- Successful bidder shall perform restoration testing biannually with the permission of CIDCO.
- Successful bidder must ensure integrity of the data returned during a restore by verifying the block data read with a check sum of the data.
- Successful bidder shall facilitate Transfer of data back in-house, either on demand or on termination of contract for any reason
- Successful bidder shall provide and implement security mechanisms for handling data at rest and in transit.
- Successful bidder must not delete any data at the end of the agreement (as per Exit Management Clause) without the express approval of CIDCO.
- When successful bidder (with prior approval of CIDCO) scales down the infrastructure services, successful bidder is responsible for deleting or otherwise securing CIDCO's Content/data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered.
- Successful bidder shall ensure prompt execution of on-demand backups & restoration of volumes, files and database applications whenever required.
- Successful bidder 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.
- The backup service must provide following capabilities.
  - Compression: Support compression of data at source before backup
  - Encryption: Support at least 128-bit encryption at source
  - Alert: Support email notification on backup job's success / failure
  - File exclusion: Ability to exclude specific files, folders, or file extensions from backup.
  - Deduplication: Provide deduplication capabilities
  - Backups should be stored in such a way that disaster at either DC or DR or both should not result in loss of backups.
- Indicative Backup plan is mentioned below.

#	Backup Type	Backup Frequency	Retention Period
1	Incremental	Daily	15 Days
2	Full	Weekly	1 Month
3	Full	Monthly	12 Months
4	Full	Yearly	7 Years

#	Restoration Policy	
1	Backup taken in last month	Once in a Month
2	Backup taken in last quarter	Once in a Quarter

5.3.6. IT Network Management Services

- The successful bidder shall perform Monitoring & Management of network links proposed as part of this solution.
- The successful bidder shall provide tools to monitor Bandwidth utilization, latency, packet loss etc.
- The successful bidder shall provide support in call logging and co-ordination with vendors for restoration of links if need arises.
- The successful bidder shall provide support for Redesigning of network architecture as and when required by CIDCO.
- Successful bidder shall give provision to monitor the network traffic of cloud virtual machine.
- Successful bidder shall offer provision to analyze of amount of data transferred of each cloud virtual machine.
- Successful bidder shall provide network information of cloud virtual resources.
- Successful bidder shall offer provision to monitor latency to cloud virtual devices from its datacenter or from outside world.
- Successful bidder must offer provision to monitor network uptime of each cloud virtual machine.

5.3.7. LAN Networking Requirements

- Local Area Network (LAN) shall not impede data transmission.
    - Successful bidder shall deploy VMs in separate security zones / network isolation layers.
    - Provide private connectivity between primary DC and DR facilities.
    - IP Addressing
    - Provide IP address assignment, including Dynamic Host Configuration Protocol (DHCP).
    - Provide IP address and IP port assignment on external network interfaces.
    - Provide dedicated virtual private network (VPN) connectivity.

5.3.8. Maintenance & Support of implemented Cloud.

- The successful bidder shall be responsible for providing 24*7*365 days' support to the infrastructure from the date of issuance of operational acceptance by CIDCO. Ensuring uptime and utilization of the cloud resources as per SLA's defined in this RFP. In the event of a disaster at DC site, activation of all services from the DR site is the responsibility of successful bidder.
- The successful bidder shall conduct vulnerability and penetration test (from a third-party testing agency which may be CERT-IN empaneled) on the cloud facility once in a year and reports should be shared with CIDCO. The successful bidder needs to update the system in response to any adverse findings in the report, without any additional cost to CIDCO.
- The successful bidder shall develop appropriate policy, checklists in line with ISO 22301, ISO 27001 & ISO 20000, PCI DSS, SOC1, SOC2 framework for failover and fall back to the appropriate DR site.

- On expiration / termination of the contract, successful bidder shall handover complete data in the desired format to CIDCO which can be easily accessible and retrievable.

5.3.9. Reports & Documentation

5.3.9.1 MIS Reports

successful bidder shall submit the reports on a regular basis in standard format. The following is only an indicative list of MIS reports that may be submitted:

#	Report Type	Frequency
1	• Summary of resolved unresolved and escalated issues / complaints. • Log of backup and restoration undertaken	Daily
2	• Summary of systems rebooted. • Summary of issues / complaints logged with the OEMs. • Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc. • Hypervisor patch update status of all servers where CIDCO Virtual Machines running.	Weekly
3	• Availability reports of Servers / Virtual machines • Consolidated SLA / Non- conformance reports • Summary of component wise uptime • Log of preventive / scheduled maintenance undertaken • Log of break-fix maintenance undertaken • All relevant reports required for calculation of SLAs	Monthly

4	• Consolidated component-wise availability and resource utilization
	• All relevant reports required for calculation of SLAs and verification of Invoices.
	• Logs and Audit Trails
	  ○ Log Access Availability (what log file entries CIDCO has access to).
	  ○ Logs retention period (the period during which logs are available for analysis).
	  ○ Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing.
		Quarterly

5.3.9.2 Alerts & Notification

- Successful bidder shall offer a fast, flexible, fully managed push notification service that lets users send individual messages or to fan-out messages to large numbers of recipients.
- Successful bidder shall offer a cost-effective outbound-only email sending service.
- The successful bidder shall provide the infrastructure performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.
- Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.
- Notifications should be triggered each time a configuration is changed.

5.3.9.3 Usage Reporting and Billing Management

- Track system usage and usage reports.
- Monitoring, managing, and administering the monetary terms of SLAs and other billing related aspects.
- Provide the relevant reports including real time as well as past data/information/reports for CIDCO to validate the billing and SLA related penalties. The reports shall consist of (not limited to):
    - Summary of resolved unresolved and escalated issues / complaints.
    - Logs of backup and restoration undertaken reports.
    - Component wise Virtual machines availability and resource utilization reports.
    - Consolidated SLA / Non- conformance reports.

5.3.9.4 Escalation Matrix & Team Member details

- The successful bidder shall provide updated escalation matrix either by email, at least once in a quarter or whenever there is a change in the escalation matrix whichever is earlier.
- The successful bidder shall also provide team member details for following teams:
    - Support Team
    - DR Drill Team

5.3.10. Disaster Recovery Services

5.3.10.1 RPO & RTO Requirements

- The successful bidder is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center meet the RPO and RTO requirements.
- 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.
- 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 and Critical Data 15 minutes
    - Applications and OS 60 minutes

- The successful bidder should offer dashboard to monitor RPO and RTO of each data type.

- There shall be asynchronous replication of data between Primary DC and DR. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to CIDCO.
- During normal operations, the Primary Cloud Data Center will serve the requests.
- In the event of a site failover or switchover, DR site will take over the active role, and all the requests will be routed to that site. 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. This is the period during which the Compute environment for the application shall be equivalent to DC.
  The installed application instance and the database shall be usable, and the same SLAs as DC shall be applicable. The use of this Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance.
- In case of any disaster, if DR is used, then charges of VM will applicable as of DC.
- The successful bidder should offer switchover and switchback of entire system and individual VMs, Applications, databases, etc. as required.
- Till a disaster (planned/ testing / drill or otherwise) is declared by CIDCO the users should not be allowed to access the IT applications from DR site (or as per discretion of CIDCO).
- The security shall be for full infrastructure i.e., Cloud-DC and Cloud-DR.
- Website and live applications (both external and internal) should be routed seamlessly from Cloud-DC site to Cloud-DR site.
- The successful bidder shall provide details of replication mechanism for (but not limited to) the following solutions:
  - Operating system
  - Database
  - Application server
  - File server
  - Email server
  - Replication Link
  - Active Directory/LDAP
- The successful bidder shall conduct DR drill one in every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DR-Cloud or vice-versa (or regular planned changes), there should not be any data loss.
- The date, time, duration, and scope of each drill shall be decided mutually between CIDCO and the successful bidder. Extreme care must be taken while planning and executing DR drills to ensure that there is no avoidable service interruption, data loss, or system damage at DC.
- The successful bidder shall clearly define the procedure for announcing DR based on the proposed DR solution. The successful bidder shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The successful bidder shall plan all the activities to be carried out during any Disaster and DR Drill. The successful bidder should intimate CIDCO least 15 working days before carrying out any DR drill.
- Successful bidder shall support in bringing the machines to login level in case of disaster / DR drills.
- RPO monitoring, Reporting and Events Analytics for the Disaster recovery solutions should be offered as part of the offering. CIDCO reserves the right the reject the Bid technically if reporting and monitoring component is overlooked by the bidder.
- The successful bidder is required to size compute and related components for DR site according to proposed solution and mention the same in solution document and include in Bill of Quantity. The successful bidder is to mandatory provide minimum RTO and RPO

mentioned in this section The successful bidder may offer better RTO and RPO and present the same in solution document.

- CIDCO shall pay the successful bidder as per 'Pay *As* You Use' model on hourly basis for the resources used at the Cloud DR site.
- Training should be provided to the staff members and System Administrator on DR.
- Bidder should provide the solution document of DR.
- The successful bidder should have proper escalation procedure and emergency response in case of failure/disaster at Primary DC.
- The successful bidder to coordinate with respective application/ product support vendor to support DR in event of disaster or for performing periodic maintenance & upgrade activities.
- The successful bidder shall provide Disaster Recovery services during the event of Disaster.
- The successful bidder will have to demonstrate the DR site to run on hundred percent for proving successful implementation of the DR site.
- CIDCO reserves the right, on its own or via a third-party auditor, to conduct overall testing at any point of time for the services delivered by the selected bidder.
- The selected bidder would be solely responsible for implementation of all tools and software at DR site. All costs including licenses/subscription/support for Software, OS, Replication Tools, etc. if any shall be borne by the selected bidder.
- Proposed solution should support Automated switchover/ failover facilities (during DC failure & DR Drills) to be provided and ensured by the selected bidder.
- The switchback mechanism shall also be automated. The selected bidder shall also provide a tool/mechanism for CIDCO cloud DC to trigger DR Failover/ switchover.
- The successful bidder shall provide support for the development of a detailed disaster recovery plan. This plan document will contain steps/procedures to switch over services to DR site in the event of invocation of disaster at DC site. Selected bidder shall also document steps for restoring services from DR site to DC site.
- In case of reverse replication, since the DR site would be acting as main site, all the necessary support to run the environment has to be provided by the successful bidder.
- Reverse Replication is necessary and envisaged when the DR site is acting as the main site. The solution should ensure consistency of data in reverse replication till the operations are not being established at the Cloud site. The RPO would be applicable in reverse replication also. The entire data should be made available for restoration at Primary Data Centre.
- The successful bidder shall develop appropriate policy, checklists in line with ISO 22301 certification for BCP.

5.3.10.2 DR Service Testing and Maintenance

- To demonstrate how the application fails over when the primary site goes down. The testing should include the:
  - Uninterrupted replication to DR servers.
  - Lag in replication due to any unforeseen errors.
  - Process of recovering from lags if any.
  - Data integrity test of DR servers.
- The successful bidder shall be responsible providing input for.
  - Devising and documenting the DR policy discussed and approved by CIDCO.
  - Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit.
- Provision for managed services for the entire DR facility will be required. Successful bidder shall provide continuous maintenance activities to support the disaster recovery site.

- Successful bidder shall provide support for all server maintenance activities. This would include periodic health check, on-demand troubleshooting, repairs, part replacement etc. from certified vendors. ITIL processes named problem, change, incident & configuration will be followed by successful bidder at DR site.
- Successful bidder should have proper escalation procedure and emergency response in case of failure/disaster at DC.
- Successful bidder may partner with respective application / product support vendor to support DR in event of disaster or for performing periodic maintenance & upgrade activities.
- The solution is envisaged for application-level recovery scalable to site level recovery based on the impact of the disaster.

5.3.10.3 Business Continuity Planning

- Successful bidder 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.
- The successful bidder 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.
- The successful bidder should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes.
- Incident response plans should be developed by the successful bidder which should involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.

5.3.11. Exit Management / Transition-Out Services

- 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 CIDCO. It is the prime responsibility of successful bidder during exit management period and in no way any facility/service shall be affected/degraded. Further, successful bidder is also responsible for all activities required to train and transfer the knowledge to CIDCO (or representative agency of CIDCO).
- 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 successful bidder. The exit management period ends on the date agreed upon by CIDCO or Three months after the beginning of the exit management period, whichever is earlier.
- At the end of the contract period or upon termination of contract, successful bidder is required to provide necessary handholding and transition support to ensure the continuity and performance of the services to the complete satisfaction of CIDCO.

5.3.10.1 Exit Management Plan

- Successful bidder shall provide CIDCO with a recommended "Exit Management SOP" 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.

- Successful bidder shall provide support to CIDCO for transferring data / applications at the time of exit management and as per the guidelines defined by MeitY in Cloud Services empanelment RFP.
- Exit Management Plan will include following but limited to:
    - 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.
    - Plans for the communication with such of the successful bidder, 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.
    - Plans for provision of contingent support to the implementation of IT Infrastructure Solution for a reasonable period (minimum one month) after transfer.
    - Method of Transition including roles and responsibilities of both the parties to handover and takeover the charge of project regular activities and support system.
    - Proposal for necessary setup or institution structure required at CIDCO level to effectively maintain the project after contract ending.
    - Training and handholding of CIDCO Staff or designated officers for maintenance of project after contract ending.
    - CIDCO will approve this plan after necessary consultation and start preparation for transition.
    - Exit management plan shall be presented by successful bidder to and approved by CIDCO.
    - Payment during exit management period shall be made in accordance with payment schedule mentioned in this tender document.

5.3.10.2 Exit Management Services

- Successful bidder shall be responsible for copy of all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to CIDCO supplied industry standard media.
- Successful bidder shall retain the data / copy of Database for 90 days and successful bidder shall ensure that there is no deletion of data for a minimum 90 days beyond the expiry of the contract without any confirmation from CIDCO. If data is to be retained beyond 90 days, the cost for retaining the data may be obtained in the commercial quote.
- The format of the data transmitted from the successful bidder to CIDCO should leverage standard data formats (e.g., OVF, VHD…) whenever possible to ease and enhance portability. successful bidder must ensure that the virtual machine format is compatible with other successful bidder, so that CIDCO can migrate from one successful bidder to other successful bidder. CIDCO should be able to export the virtual machine from successful bidder cloud and use that anywhere. successful bidder shall give provision to import cloud VM template from other successful bidders.
- Successful bidder shall necessarily support for termination of network connectivity to / from other successful bidders (within India) if required.
- Successful bidder shall ensure that all the documentation required by CIDCO for smooth transition (in addition to the documentation provided by the successful bidder) are kept up to date and all such documentation is handed over to CIDCO during regular intervals as well as during the exit management process. Also ensure that all the documentation required for smooth transition including configuration documents are kept up to date.
- Post exits all the data content should be removed to ensure that the data cannot be recovered.

- Successful bidder shall address and rectify the problems with respect to migration of CIDCO application and related IT infrastructure during the transition.
- Successful bidder shall decommission and withdraw all hardware and software components after the completion of the contract period and formally close the project. This process will be initiated 6 months before the ending of the project contract.
- At any time during the exit management period, the successful bidder will be obliged to provide an access of information to CIDCO and / or any Replacing Vendor in order to make an inventory of the Assets (including hardware / Software / Active / passive), documentations, manuals, catalogs, archive data, Live data, policy documents or any other material related to implementation of IT Infrastructure Solution for CIDCO.
- Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule

5.3.12. Connectivity and Customer Premises Equipment features.

5.3.12.1 General Requirements.

- The Successful Bidder should provide 24X7 support for services and components mentioned in Scope of Work and Bill of Material.
- The successful bidder should provide 24X7 monitoring services and components mentioned in Scope of Work and Bill of Material.
- The successful bidder shall assign a service manager for the duration of the Contract. This resource should be the "Single point of contact" for all service-related matters for CIDCO and should be able to respond within the designated service window. The proposed "Service manager" should be a multi-skilled professional and supported by back-end support as required.
- Successful bidder shall be responsible for DNS / reverse DNS changes in the Internet connectivity as and when required.
- Successful bidder should provide a report based on the IP and application high consumption bandwidth.

5.3.12.1. Manage DNS Security Services

- Provide Authoritative Domain Name Service with 100%availability.
- Solution should support unlimited DNS records, sub-domain and DNS Queries/per month.
- Global propagation of DNS record updation in < 5 seconds
- Ability to configure custom TTL value per DNS record.
- Should have option to use custom DNS hostnames.
- Support auto record updation via health check results from load balancing functionality
- Online DNS Query Analytics by response codes, record type, geography,
- domain.
- Ability to download logs to be ingested in SIEM/parsing tools.
- RBAC for DNS management
- MFA and SSO support
- Support CNAME record at the apex level.
- Unmetered DDoS attack mitigation on DNS
- Should run over ANYCAST network.
- Should support DNS resolution across all the POPs and not limited to specific. POPs
- Support for IPv4 and IPv6 address
- Should comply with RFC8482
- Uptime Service Credit to be offered.

- Subscription to be based on root domain and not sub-domains.
- Support for DNS configuration via API
- DNS Analytic Dashboard with time range from 30 min to up to 1month-
- Queries by Response code Queries by Record type
- Top Queried DNS Record DNS Query by POP

5.3.12.2. VPN Service

The successful bidder should provide a VPN solution to the enable CIDCO's field offices to access CIDCO applications hosted on cloud in a secure manner. The solution should enable the field offices with poor connectivity/ no connectivity to access CIDCO's applications and provide services to citizens.

5.3.13. Cloud Security Requirement

The successful bidder should ensure complete security requirements for the Government Community Cloud hosting of CIDCO with suitable security arrangements through SaaS model (Security as a Service) as per MeITY guidelines. successful bidder shall provide end-to-end security services to meet IT security challenges for the infrastructure based on the proven frameworks and security best practices. It is vital for complete security that the processes and technology which shall support the Information Security function are proven and adhere to standards.

It is envisaged that the security operations shall be centralized, structured, and coordinated and shall be responsive resulting in effective threat prevention and detection helping the deployed cloud solution to be secure from attackers. The Information Security functions shall respond faster, work collaboratively, and share knowledge more effectively. The proposed cloud solution shall have multiple security layers to secure the infrastructure from threats. successful bidder shall propose and provide security solutions that may not be mentioned in the RFP but are required as per the guidelines of MeITY.

Successful bidder shall provision for following security solutions (not limited to):

- Next-Generation Firewall (NGFW) having minimum 1Gbps threat-prevention throughput (all features enabled).
- Web Application Firewall for OWASP (Open Web Application Security Project) Top 10 protection
- IPS (Intrusion Prevention System)/IDS (Intrusion Detection System)
- HIPS (Host Intrusion Prevention System)
- Malware Analysis - successful bidder shall conduct analysis of newly discovered malware to uncover its scope and origin.
- DDoS (distributed denial-of-service) service - successful bidder would offer DDOS Protection to protect the cloud infrastructure and application from well-equipped attackers. Minimum mitigation of 1 Gbps.
- Anti-Virus - This Service includes virus detection and eradication, logon administration and synchronization across servers, and support for required security classifications.
- IAM (Identity Access Management) - The User Management services shall include Directory Services for which comprises of the following services:
    - Domain management
    - Group management
    - User management
    - Implementation of domain policies and standards etc.

  - Directory services are to be used by CIDCO.
  - Role Management
  - Access Management
  - Multi-Factor Authentication
  - Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.
- The successful bidder shall also propose for Security Information and Event Management (SIEM) solution supporting threat detection and security incident response through the real-time collection and historical analysis and correlation of security events from a wide variety of event and contextual data sources. It shall also support compliance reporting and incident investigation through analysis of historical data from these sources.
- VAPT (Vulnerability Assessment and Penetration Testing) – The successful bidder shall conduct vulnerability and penetration test (from a third-party testing agency which has to be CERT-IN empaneled) on the Cloud facility every year and reports shall be shared with CIDCO. The successful bidder needs to update the system in response to any adverse findings in the report, without any additional cost to CIDCO.
- Security solution during data in transit and at rest
- Anti-APT (Advanced persistent threat) Solution – It shall Identify, and analyses targeted and unknown files for more than 100 malicious behaviors. IT shall generate and automatically deliver protection for newly discovered malware via signature updates.
- NTP (Network Time Protocol) - Clock Synchronization - The provisioned NTP solution should have the capability to synchronize clock with systems like network equipment, voice systems, servers, appliances, desktop systems etc.
- 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 and be maintained & implemented by Cloud service provider (successful bidder).
- CIDCO will perform physical audits at the data centre and will require access to CIDCO's infrastructure as and when required by CIDCO.
- CIDCO has right to conduct 100% GCC/VPC compliance with the help of any third-party agency (appointed by CIDCO) in the Data Center(s) on the infrastructure provided by the bidder.
- 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.
- Data shall not leave the Indian boundaries and data residing within Cloud shall not be accessed by any entity outside the control of CIDCO.
- Cloud service 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.

5.3.13.1. Web Application Firewall Services

- The Web application firewall should address Open Web Application Security Project (OWASP)Top Ten security vulnerabilities such as SQL Injection, Cross Site Scripting (XSS), Broken Authentication and Session Management.
- The Proposed solution must be cloud based / off premises. WAF Services should be managed OEM.
- The solution should prevent the following attacks (but not limited to):
  - Brute force */DDOS*

  - Access to predictable resource locations
  - Unauthorized navigation
  - Web server reconnaissance
  - HTTP request format and limitation violations (Size unknown method, etc.)
  - Use of revoked or expired client certificate
  - File upload violations
- Total number of Applications to be supported: 20 which must support up to 50. with future scalability
- WAF should support multi node operations simultaneously.
- Proposed solution should protect against content modification attacks like URL. rewriting, Cookie signing, encryption, etc.
- The Web Application Firewall should have Reputational Base Service which can provide a near real time live feed of know attack.
- Proposed solution should be capable of detecting web-based malwares and protect the web application against DoS attacks.
- The proposed service provider must have hosted WAF solution within India. Datacenters
- The proposed cloud based WAF solution is required to support applications. hosted at Cloud Datacenter, Cloud Disaster Recovery site and On- Premise DC (Andheri HQ) of CIDCO
- The cloud based WAF must have dedicated throughput up to 50 Mbps on all locations (Cloud DC & DR, On- Premise DC with on demand scalability. CSP/MSP to size throughput accordingly.
- 24 x 7 support and monitoring and management to be taken care by the service. provider with configuring rules and policies in discussion with the CIDCO team.
- Required Patching and necessary upgradation to be taken care by the service. providers team
- The solution must support IPv4 and IPv6 capability.
- The proposed WAF solution shall be capable to provide security logs can be shared with SOC.
- The proposed solution must be PCI DSS compliant.
- Real time monitoring and dashboard capability
- Every POP should have full capability of security services like DDOS, Firewall,
- WAF, CDN, Load Balancing, etc.
- Should operate on ANYCAST network
- 100% Uptime SLA
- Uptime Service Credit to be offered.
- Should be IS02V001:2013, SOC2 Type II, PCI 3.2.1, HIPPA, GDPR, ISO 17018:2014, ISO 27017=2015, OHSAS certified
- Subscription to be based on root domain and not sub-domains.
- Should come with recommended WAF policy and action set and also provide ability to set custom actions.
- Should support Opportunistic Encryption
- Should offer End-to- End TLS/SSL encryption between Client and Server
- Should support TLS 1.2 and 1.3 with ability to enforce minimum TLS version.
- Should have ability to provide customize TLS Protocol like disabling TLS 1.0 and TLS1.1
- Should have ability to enforce HSTS policy.
- Ability to redirect all requests with scheme "http “to "https."
- Support automatic *HTTPS* Rewrites

- Ability to add custom SSL certificates.
- Support for OWASP Core Ruleset with ability to selectively set actions on OWASP rule set by category i.e., Bad Bots, HTTP Policy, Protocol Violations, Request Limits, etc.
- Should provide WAF rule sets for Drupal CMS,Joomla CMS, Wordpress CMS,Magento CMS,Plone CMS,Flash, PHP, Whmcs with ability to set enable/disable each rule and set action.
- Should support Action as Default (Recommended), Disable, Simulate, Block, Challenge
- Ability to have custom WAF rules.
- Ability to block traffic based on User-Agents
- Ability to block specific URL from specific IP Address, IP Subnet with rule priority.
- Ability to enforce rate limit on a URL pattern for the source ip within a defined time interval.
- Ability to set select Inbound traffic based on - Cookie, Country, Continent,
- Hostname, IP Address, Referrer, Request Method, SSL/HTTPS, URI Full, URI, URL Path, URI *Query* String, *HTTP* Version, User-Agent, X-Forwarded-For, Known Bots, Threat Score
- Set condition to selected Inbound traffic as - equal," does not equal, greater than, less than, greater than or equal to, less than or equal to, is in, is not etc.
- Ability to set AND/ OR condition across multiple rule sets.
- Action for selected Inbound traffic can be - Block, JavaScript Challenge, Allow, Bypass, Log
- Ability to save the rule in draft mode without applying
- Configuration changes to be enforced in < 30 seconds across the provider platform.
- Ability to set rules to selective bypass WAF inspection to a particular URL with support for wildcard as well.
- Ability to selectively set SSL settings to Off, Flexible, Full, Strict based on URL. with support for wildcard as well
- Ability to set http headers for True Client IP
- Ability to set http headers for IP Geolocation
- Ability to set custom error pages.
- Ability to serve static page in case of origin web server is unavailable.
- Should offer IPv6 IP address to protected applications.
- Support for Web sockets
- Support for pseudo IPv4 address when end client support IPv6 and protected.
- web application supports IPv4 only.
- Should have support for Load Balancing between multiple protected servers.
- Analytics Dashboard with time range from 30 min to up to 1month-
- Requests by Country/Region, Bandwidth Served, Unique Visitors, HTTP Status Codes
- Threats - Total threats, By Top Country/Region, Top Threat Types SSL - Volume of traffic Served over SSL
- Provider to provide logs for ingestion in Successful Bidder EM
- WAF logs for real-time viewing on portal.
- RBAC for management portal
- Support 2FA for accessing management portal.
- No Hardware & Software to be installed at origin web server for the provision. of the services
- Should support Positive security model.
- Manual configuration
- Should support Negative Security Model
- Signature Based

- Rule Based
- Once the vendor patches the identified vulnerabilities, a final targeted scanning. for those specific vulnerabilities must be carried out under advice to the Customer.
- Should provide Service Level Commitment of 99.999% at least with Service Credits
- Should have ability to perform load balancing between different origin IP address in either Active-Active mode or Active-Standby mode.
- Should be able to provide User Defined Customized Reporting and compliance reporting.
- Should support HTTP2.0 gateway for all the HTTP/s applications.
- Should have Geo-IP Blocking capability self-service.
- WAF should provide a real-time single management console to manage multiple WAF instances protecting multiple websites. The dashboard should contain data such as top attacks view, traffic monitoring view etc.
- Should be ICSA lab certified.
- Should be NSS Lab certified.
- Should not have any restriction on no. of rules.
- Should have 24x7x36Sdays WAF-attack detection and alerts capability.
- Pro-active Policy tuning and configuration management should be in place.

5.3.13.2. DDOS as a service

- The proposed solution should be provided on cloud-based model/ off premises. DDOS Service should be managed by OEM.
- The proposed solution should detect and mitigate both traditional network layer.
- DDoS attacks and more advanced application layer attacks
- The proposed solution or service provider must have scrubbing farms across all the major countries. Please specify the locations. This feature to mitigate at the source.
- Minimum capacity for required for mitigation of 1 Gbps.
- Scalability should be available as and when required.
- Fixed billing model based upon detection and mitigation.
- The proposed solution should protect against zero-day attacks.
- The proposed solution must be built on stateless analysis filtering engine.
- The proposed solution should detect low & slow application-layer.
- DDoS attacks and specially crafted packet attacks.
- The proposed solution must support a latency of less than 80 microseconds, which must be clearly documented in the data sheet.
- The proposed solution must detect rate based and connection exhausting attacks against SSL/TLS
- The proposed solution should have following capabilities:
    - DDoS Protection from active botnets
    - DDoS Protection from active
    - DDoS complains based on IP reputation.
    - Advanced web crawler service
    - GeoIP Tracking Domain and IP reputation to block threats.
- The proposed solution should prevent suspicious outbound traffic for threats and blocking malicious traffic
- The proposed solution must be able to block Invalid Pockets (including checks for Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad Tep / UDP

Checksum, Invalid TCP Flags, Invalid ACKNumber) and provide statistics for the packets dropped.

- The proposed solution must support rate- limit protections for UDP flood detection, fragment flood detection, private address blocking and multicast blocking.
- The proposed solution must be able to detect sources that send excessive amounts of traffic according to configurable thresholds, and then must provide the flexibility to place those sources on the temporary blocked hosts list (rate base blocking)
- The proposed solution must be able to regularly activate new defense techniques from regularly updated attack signatures that are maintained by the vendor's research team via 24x7 monitoring of the Internet to identify the most significant and recent botnets and attack strategies.
- The proposed solution must provide the ability to block bot- originated traffic according to system- supplied signatures.
- The proposed solution must be able to drop packets of specified TCP ports with payloads matching or not matching a configurable regular expression.
- The proposed solution must support the ability to blacklist a host, country, domain, URL.
- The proposed solution must be able to limit the number DNS Queries per second by a user-configurable rate.
- The proposed solution must be able to detect and drop malformed HTTP packets that does not conform to RFC standards for request headers, and then facility to blacklist the source hosts.
- The proposed solution must provide the ability to block bot- originated traffic according to system- supplied signatures.
- The proposed solution must provide summary reporting of user defined Top IP Sources and Destinations
- The proposed solution must display summary reporting by Country classification.
- The proposed solution must display statistics on the amount of dropped and passed traffic.
- The proposed solution must display real- time protection statistics on dropped and passed traffic in bytes and packets, with rate statistics in bps and pps.
- The proposed solution must support the generation of pdf reports containing.
  the detailed statistics and graphs for any user defined entity from the solution on real time basis.
- The proposed solution must support the generation of e-mail reports with the detailed statistics and graphs for any user defined entity from the solution.
- Established provider operating across more than go countries and scrubbing centers across the globe and with 5Tbps of mitigation capacity.
- Should operate on ANYCAST network.
- 100% Uptime SLA
- Uptime Service Credit to be offered.
- Should be IS027001:2013, SOC2 Type II, PCI 3.2.1, HIPPA, GDPR, ISO 17018:2014, ISO 27°17:2015, OHSAS certified.
- Unmetered DDoS attack mitigation for protected applications
- Mitigation of DDoS attacks against layers 3, 4, & 7
- Subscription to be based on root domain and not sub-domains.
- Offer prioritized IP ranges and routing, ensuring maximum speed and availability.
- Protect TCP*IUDP* based applications from Volumetric DDoS attacks in Always ONmode
- Designated Customer Success Manager
- Designated Solution Engineer
- Time to Detect and Time to Mitigate to be less than 10 sec. without any manual intervention.

- Should provide API access for automation.
- RBAC for management portal
- Support 2FA for accessing management portal.
- No requirement of Client owned IP Pool for protection.
- WAF and DDoS should be from same OEM so that there is a tight integration between both in Terms of integration and security.
- For Cloud based WAF and DDoS there should not be separate traffic redirection to be configured by Customer
- DDoS Provider should have local scrubbing center to mitigate volumetric DDoS.
- Attack and traffic should not go outside India.
- Should have support mechanism to reach support team within 10 minutes of response time with Emergency hotline service capability which should be available 24x7X365days.

5.3.13.3. Endpoint Security (Endpoint Detection and Response and Anti Malware)

- The proposed solution should provide complete server protection (Windows and Linux). It should have centralized management,
- The antivirus solution Should Support Multi -Platform operating system (Windows, Mac, Linux) and the same should be managed from a Centralized Management Console
- The antivirus solution should have single, ·Configurable Installation with centralized configuration & policy management.
- Solution should ensure that all managed endpoints are updated in scheduled intervals and shall also ensure that there is no impact on the performance of endpoints during the updates.
- The proposed solution should have solution should have-single agent for Antivirus and Anti-spam, Firewall, Intrusion prevention, Web Reputation, File
- Reputation, Real Times Analysis, Device Control.
- Must protect against all kinds of viruses, Trojan horses and worms including boot sector, master boot sector, memory resident, file multipartite, macro etc.
- Must support exclusion list by file extensions.
- Anti-Virus Software must have the capability to clean; Quarantine or- delete Viruses and should be able to detect new classes of viruses by normal virus definition update mechanisms.
- Must have heuristic scanning to allow rule, - based detection of unknown viruses.
- It should give a pop - up alert box to the user to disinfect, delete, quarantine or block access to that file whenever an infection is found in it (user defined)
- It should give a wop- up alert box to the user to disinfect, delete, quarantine or block access to that file whenever an infection is found in it (user defined)
- Administrator should be able to lock down all anti-virus configurations at the desktop & User should be prevented from being able to uninstall the anti-virus software.
- The solution must have real time scanning, local scanning, scheduled scanning.
- The solution must provide the logs for real time scanning, local scanning, shell scanning, general events like signature updates and must be integrate with 3rd party Successful Bidder EM.
- Antivirus solution should have a Live web protection module Integrated into existing endpoint agent with no endpoint configuration required to Blocks.
- URLs that are hosting malware and Should Support all major browsers - IE, Firefox, Safari, Opera, Chrome
- Patching and upgradation and monthly report to be shared with the CIDCO team for review.
- Management servers must be configured in High availability mode. Also, at DR- site for failover.

5.3.13.3.1. Endpoint Detection & Response (EDR)

- Solution should automatically detect and confirm multistage zero-day malware and targeted attacks without prior knowledge of the malware.
- The solution must be able to accurately identify malware and maintain a very low false-positive rate via the use of global file reputation. It should also allow for administrative intervention for any subjective files and/ or if the company deems a file as malicious.
- To support Indicators of Compromise (IOCs) searching and file hunting, the solution must support minimally MDS and SHA2 file hashes.
- Solution should have the ability to report the Source IP) Destination IP, C&C,URL, Malware class, executable run, used protocols and infection severity of the attack.
- Solution should provide the ability to locate and download the infected malware sample.
- The solution should allow controls over files sent for sandboxing and should also have option to do sandboxing on- premises.
- Endpoint agents must be able to be controlled on and off the corporate network for the purposes of detection, triage and containment.
- The Advanced Threat Protection solution must be able to take inputs for custom indicators of compromise.
- The proposed solution should support Endpoint quarantine from network and bring back the Endpoint after remediation using ATP management platform.
- The Solution should support summary reports of enterprise malware events, breaking down malwares by type, host, and activity.
- The Solution should support immediate analysis as to whether the malware maps to a previously known or unknown threat.
- Endpoint Detection &Response solution should be compatible to work on any Endpoint Security/Antivirus solution and should be independent of any Antivirus technology.
- The proposed solution must gather security information from the host including its network shares, patch level, and running Windows tasks.
- The proposed solution must not rely on Anti-virus signatures in order to return an analysis and indicate if an endpoint is compromised.
- The proposed solution must analyze Windows internal structures for alteration and consistency.
- The proposed solution must search for kernel and user mode hooks in SSDT, IDT, AT/EAT, and IRP_MJ.
- The proposed solution must be able to analyze and report all files using MDS, SHAl, and SHA 256 hash methods.
- The proposed solution must be able to provide a complete environmental correlation that shows the clients and the number of systems where the identified malicious file was found.
- The proposed solution must be able to track and monitor host activity from time of last boot and correlate an infected file back to the original malware executable.
- The solution must support the ability to exclude applications or files from exploit detection.
- The proposed solution must be able to integrate with Successful Bidder EM solutions at CIDCO to cross reference against TIPs, I0Cs feeds & custom IOCs , to help respond to co-relate & respond.
- The proposed solution must allow building custom 10Cs set and using it to correlate against suspicious files and Solution EDR should have capability to search for Intel feeds like malicious Hashes, Domain & IP addresses.
- The proposed solution must be able to provide visibility to the digital signatures of executables.

- The proposed solution must be able to capture triage summary automatically, to provide. a quick summary and have capability to capture files, memory, detailed triage and disk for forensics,
- The proposed solution must be able to identify & hunt TIPs, 10Cs on the following OS.
  - Windows Server 2012 and higher
  - Windows 10 and higher
  - Linux (Redhat, CentOS, etc.)
- The proposed solution must allow remote upgrade of the agents running on the endpoint clients.
- The proposed solution must allow remote removal of the agents running on the endpoint clients.
- The proposed solution must encrypt the communication between the agents and the management server.
- The proposed solution must encrypt the communication between the management console and the management server.
- The proposed solution must be able to set scan priority on the host to prevent performance degradation on the client (low priority scan option).
- The proposed solution must be able to remotely block the infected endpoint without any dependency on 3rd party solutions.
- The proposed solution must be able to remotely respond to the infected endpoint without any dependency on 3rd party solutions.
- The proposed solution must be able to report on the client status:
  - Scan in progress
  - Offline
  - Idle
- The proposed solution must be able to provide a detailed report of individual.
- client and must consist of the following information, at minimum:
  - Hostname
  - Last Scan
  - Any pending scan requests.
  - IP Address
  - Username logged in.
  - Agent installed date.
- The proposed solution must be able to report on the preliminary status of analyzed host machines:
  - Compromised
  - Suspected Compromised
- The proposed solution must be able to export reports as HTML or PDP or CSV.
- The scan report must provide a preliminary assessment of the state of the client. at the end of the scan, accompanied with supporting detail to support the result.
- The solution should support agent capping for CPU and memory utilization.
- The Solution client should be deployable from patch management solution or through AD.
- Solution should be able to upgrade the agents remotely.
- The proposed EDR solution must integrate with 3rd party Successful Bidder EM for compliance and auditing purpose.
- The proposed EDR Solution must integrate with propose Cyber Automation Solution to automate, orchestrate and respond to endpoint related alerts.
- The EDR solution must be able to detect IOC based, file less malwares which does not depend on any signatures.

- The proposed solution must provide continuous detection and response activities for advanced threats. The local cache on Endpoint agent should allow to inspect and analyze present and past alerts at the endpoint.
- The proposed solution Endpoint agents must be able to be controlled on and off the corporate network for the purposes of detection, triage, and containment.
- The proposed solution must be capable of detecting data exfiltration.
- Endpoint solution must help Security Analysts to define custom indicators of compromise for DNS, File & Network Connections.
- The solution must be capable of linking networking processes with parent processes.
- The solution must be able to provide a recent historical listing of processes.
- The solution must support to display a recent command history.
- The solution must support to read and display machine logs.
- The solution must support to show a local login history.
- The solution must allow grouping of endpoints into host sets based on distinguishing attributes. It must also be able to identify and label high-value hosts.
- The solution must be able to throttle the triage collection if a widespread compromise or false positive is generating inordinate number of triage requests.
- The solution must be able to differentiate between presence and execution indicators of compromise.
- Solution should be able to terminate malicious payload at run time for exploited applications as well as it should provide capability to terminate exploited application based on behavioral analysis.
- Security vendor must have their own integrated exploit detection and prevention engine without relying on 3rd party tools.
- The solution must be able to automatically kill exploited applications or automatically prevent any payload from exploited application to run.
- End-user shall be notified of automatically killed applications and payloads ensuring seamless user experience.
- The solution must support the ability to exclude applications or files from exploit detection.
- Solution must be able to drill into system activity during a specific incident time window to determine the source of the threat and possible data exfiltration or lateral movement.
- Solution must be able to mitigate the impact of a compromised system with network isolation using workflow driven containment in order to prevent lateral spread.
- *The* solution must have a two- stage process for containment requests, with the ability to separate the requestor and approver roles.
- The solution must support containment of suspected hosts while maintaining access to the Endpoint Forensics solution for investigation as well as other whitelisted resources used for infestation or remediation.
- The solution must be able to exclude mission-critical hosts from containment, ensuring enterprise-wide disruptions are minimal.
- The solution shall support end-user notification when containment is enforced.
- Solution must provide an easy-to-use interface and require no more than an entry level SOC analyst and/or IR responder skillset to operate.
- Solution should provide Simplified Triage View where Responders can see timeline events such as Files written on endpoint, Registry.
- Added, Outbound Network connections, process executed. This should help Incident Responders to understand scope of attack.
- Endpoint agent should record real time events listed below and should perform.
  a triage collection for forensic analysts to investigate those endpoints:

  - Process starts and end events.
  - DNS lookups
  - Network connections
  - URL accesses
  - Image loads'
  - IP address changes
  - Registry accesses
  - File writes
- Solution should be able to automatically generate forensic package upon detection of a threat or IOC match for deep level forensic by Incident Responders.
- Solution should be able to detect attacks & alert using methodology indicators such as understanding attacks loaded into memory to steal passwords or PowerShell commands usage with arguments run by attacker for stealing credentials.
- In assisting with an investigation, the agent can remotely send memory dumps, files, running processes, services, drivers, dll's, open handles, and network information.
- Solution should provide capability to SOC analyst to acquire malicious file remotely for analysis.
- Solution must provide the following hunting/searching capabilities across all agents:
  broadly search for known malicious behavior proactively "Hunt" for suspicious activity
  comprehensively investigate compromised endpoints search for all evidence of advanced intrusions, not just malware
- Hunting and Search features across endpoints should be available around key metrics interesting for Security Analysts related to Browser Name, Browser Version, Cookie Flags, Cookie Name ,Cookie Value ,DNS Hostname ,Driver Device Name ,Driver Module Name ,Executable Exported DLL Name, Executable Exported Function Name, Executable Imported Function Name Executable Imported Module Name ,Executable Injected, Executable PE Type, Executable Resource Name ,File Attributes ,File Certificate Issuer, File Certificate Subject, File Download Mime Type, File Download Referrer, File Download Type, File Full Path, FileMDSHash, File Name, File SHAI Hash, File SHA2S6Hash, File Signature Exists, File Signature Verified, File Stream Name, File Text Written, HTTP Header, Host Set, IP Address, Local IP Address, Local Port, Parent Process Name, Parent Process Path, Port ,Port Protocol, Port State, Process Arguments, Process Hidden, Process Name, Registry Key Full Path,
  Registry KeyValue Name, Registry *Key* Value Text, Remote IP Address, Remote Port, Service DLL ,Service Mode, Service Name, Service Status, Service Type, Size in bytes, Task Flag, Task Name, Task Status, Timestamp - Accessed, Timestamp - Changed,Timestamp - Created, Timestamp - Event, Timestamp - Last Login Timestamp Last Run, Timestamp - Modified, Timestamp . Started, URL, Username, Web Page Title, Windows Event ID, Windows EventLog Type, Windows Event Message,
- The solution shall support concurrent searches across all endpoints.
- Solution must provide the following live response capabilities:
  - Investigative visibility into all traces of activity on any endpoint suspected of being compromised.
  - Replay the entire timeline of an advanced attack.
  - Capture and review actual "hands on the keyboard" activity by intruders
- Perform Full forensic activities to thwart intruders attempt to hide or avoid detection and investigation. (e.g., Raw disk access, live memory analysis, rootkit detection, known persistence locations monitoring, etc.)
- The solution must be able to acquire detailed volatile/non-volatile forensics metadata on System Information, File System, Drivers, Kernel Hook Detection, Persistence (e.g., autoruns), Registry, Event Logs, Processes, Browser, Tasks, Network, Services, real- time

events.

- The solution must be able to acquire raw Files, Full Disk, Process memory, Full memory and driver memory images.
- Solution should provide manual remediation capabilities to administrators to remotely connect to endpoints and execute commands.
- Communication channels should securely communicate with endpoints to eliminate the need to configure any additional firewall rules or ports for the module to be able to perform normal operations.

5.3.13.3.2. Anti-Malware Protection

- Solution should have anti-malware scanning engine as well as malware. prevention and remediation. It should offer functions like Quarantine file,
- Clean file & delete file automatically.
- Option should be available to turn on & off malware detection & remediation.
- Single agent solution should provide EDR, malware detection, unknown exploit prevention & malware remediation capabilities.
- Solution should provide capability to exclude several hosts as required as part of malware scanning.
- Solution should provide option to schedule On Demand scan of full disk, quick scan, active-memory scan.
- Solution should provide on access malware on files accessed over your network during file read only operations, file write only operations, or on file read and write operations.
- Malware Remediation engine should be able to remove artifacts created by the malware and revert changes the malware made to other files or registry entries i.e., referred to as removing malware traces. It should work as per below indicated scenarios:
- If the infection appended infected code to user files, attempts should be made to clean the infection from the files.
- If the attempt to clean the files fails, the files remaining on the endpoint should be acquired for analysis.
- If the infection introduced new files to the endpoint, attempts should he made to delete them.
- If the infected files are locked and cannot be deleted without rebooting the endpoint, a notification message should be displayed on the endpoint.
- Malware protection behavior should be controlled using global and exception policies. These policies should allow to turn the detection and quarantine functions on and off, to control the remediation actions taken when malware is detected, and to exclude specific types of malwares, specific processes, specific files and folders, specific MD5 hashes, and even specific group of hosts from detection and remediation.
- Malware definition updates should be downloaded to the Agents from the controller appliance or from the Internet or with fall back options and should be configurable from GUT.
- Endpoint security solution should have machine learning capability to detect unknown malwares.
- Endpoint Security Solution should provide capabilities to integrate with on-premises sandboxing to submit suspicious samples for further analysis.
- Endpoint Security Solution should have capabilities to identify unique file executions on an endpoint and report these executions and should have capabilities to submit it to local Sandbox for further analysis, if found malicious it should gather related evidence/artifacts.
- Endpoint Security should prevent attackers from obtaining access to credential data or key material stored within the Windows.

- Local Security Subsystem Service (LSASS) process, thus protecting endpoints against common credential theft attacks.
- Solution should block User Account Control (UAC)bypass attacks like Token Manipulation, Process Masquerading, Environmental variable hijacking, Shell command hijacking, COM handler hijacking, Program Output Abuse.

5.3.14. Security Controls

- Successful bidder shall provide adequate security controls not limited to the measures as described below:
    - Secure Access Controls
        - The system shall include mechanisms for defining and controlling user access to the operating system environment and applications. Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.
- Authorization Controls
    - A least-privilege concept such that users are only allowed to use or access functions for which they have been given authorization shall be available.
- Logging
    - Logs must be maintained for all attempts to log on (both successful and unsuccessful), any privilege change requests (both successful and unsuccessful), user actions affecting security (such as password changes), attempts to perform actions not authorized by the authorization controls, all configuration changes etc. Additionally, the access to such logs must be controlled in accordance with the least privilege concept mentioned above, so that entries may not be deleted, accidentally or maliciously.
- Hardening
    - All unnecessary packages must be removed and/or disabled from the system. Additionally, all unused operating system services and unused networking ports must be disabled or blocked. Only secure maintenance access shall be permitted, and all known insecure protocols shall be disabled.
- Malicious Software Prevention
    - Implementation of anti-virus software and other malicious software prevention tools shall be supported for all applications, servers, data bases etc.
- Network Security
    - The network architecture must be secure with support for UTM, Firewall and encryption. The system shall also allow host-based firewalls to be configured, as an additional layer of security if the network firewall were to fail.
    - Cloud services shall be provided on a 10Gbps scalable to 50Gbps network connectivity between the server and Storage and Network. Cloud service shall be able to support multiple (primary and additional) network interfaces. The proposed data center shall be isolated from failures in other data centers. As mentioned in RFP successful bidder proposed data center shall be connected with low latency and in-expensive network connectivity.
    - Cloud service provider should be able to configure the secure network over an internet like IPsec VPN tunnel or SSL VPN.
    - Cloud services shall provide a web interface with support for multi-factor authentication to access and manage the resources deployed in cloud and also

provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing.

- Information Security: Log Monitoring and Correlation
    - All Servers / sub systems / network devices / appliances as proposed shall have capability and throw logs to the log server. The Logs and events generated by VMs, applications, DB, network, security component / devices of the system shall be monitored. successful bidder must provide a Security information and event management (SIEM) solution for the same which shall be capable to provide various security alerts, events, logs generated from various IT infrastructure (Hardware/Software) components. successful bidder would need to ensure the IT security compliance and therefore monitor the threats/logs generated by various equipment's / sub systems.
    - The successful bidder would need to store the events for minimum 6 months. Also, successful bidder will be required to scale the storage if the existing storage space is full.

5.3.15. Cloud Security Administration

- The successful bidder shall provide 24x7x365 managed services for the entire security stack protecting the CIDCO environment. successful bidder shall be responsible for managing configuration and patch management, vulnerability scanning, protecting data in transit and at rest, managing credentials, identity, and access management etc. The activities include:
    - Appropriately configure the security groups in accordance with the Security policies
    - Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.
    - Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.
    - Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity.
    - Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by their Government Agency's policies.
    - Review the audit logs to identify any unauthorized access to the government agency's systems.
    - The protection from unauthorized usage, detection of intrusions, reporting as required and proactive prevention actions are to be provided by successful bidder.
    - Service Component Administration
    - User and Password Control
    - Check and maintain access control
    - Routine connection tests
    - Change & Configuration Management
    - IP / Port / Zone Configuration
    - Firewall policy / IPsec VPN / SSL VPN configuration
    - NAT / PAT configuration
    - Multicast configuration
    - Antivirus / IPS Signature update, when released by vendor.
    - Fault Management
    - Response to alerts generated by systems or problems reported.
    - Troubleshooting, root cause analysis (RCA) and identification of problem area
    - Resolution of problems through configuration changes/ re-installations / replacements
    - Escalate hardware failures to hardware vendor.

- Assist hardware vendor to Identify problem area (by log collection & reboot)
- Log Storage: Store critical logs in shared Syslog server for retention period of 90 days
- Configuration backup: Take incremental configuration backup daily for retention period of 90 days and Restoration of configuration when required.
- Trouble ticket logging, update, and closure
- Managing configuration and security of Demilitarized Zone (DMZ) Alert / advise CIDCO about any possible attack / hacking of services, unauthorized access / attempt by internal or external persons etc.
- Incident Response - The successful bidder should have policies and procedures in place for timely detection of vulnerabilities within organizationally owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. The successful bidder/successful bidder must also have policies and procedures in place to ensure timely and thorough incident management, as per established IT service management policies and procedures. The Solution shall be complied with ITIL (Information technology Infrastructure library) standards.
- Governance & Risk Assessment - The successful bidder should have organizational practices in place for policies, procedures and standards for application development and service provisioning as well as design, implementation, testing, use, and monitoring of deployed or engaged services in the cloud.

5.3.16. Deployment of Resources

Below mentioned resources will be working from their own office on website redesign, development and implementation. However, successful bidder shall deploy 3 senior software developers separately within 15 days from the issuance of LOA for operating and maintaining the existing website till the new website goes live.

1. Migration activities for data and application services
2. Website redesign ,development and implementation
3. Annual maintenance of website and cloud services.

#	Role	Min. Qualification & Experience	Number of resources
1	Project Lead	• B. Tech / B. E in CS/IT/EE or MCA; with 7 years of IT experience Or Any Graduate with9 years of e-Governance Experience	1
2	System/cloud Administrator	• B. Tech / B. E in CS/IT/EE or MCA; With 4 years of IT experience and having certifications like MCSE/RHCE/RHEL Or Any Graduate having 7 years of IT experience with certifications like MCSE/RHCE/RHEL	1
3	Senior Software Developer	• B. Tech / B. E in CS/IT/EE or MCA; With8 years of relevant IT experience Or Any Graduate having 7 years of IT experience out of which minimum 5 years should in Government domain.	2
4	Software tester	• B. Tech / B. E in CS/IT/EE or MCA; With 8 years of relevant IT experience Or Any Graduate having 7 years of IT experience	1
5	Software Developer or UI/UX Developer	• B. Tech / B. E in CS/IT/EE or MCA; With 2 years of relevant IT experience Or Any Graduate having 5 years of IT experience	1
6	Database Administrator	• B. Tech / B. E in CS/IT/EE or MCA;with 4 years of IT experience & certifications like OCA-DBA/OCP- DBA/MCDBA Or Any Graduate having 7 years of IT experience with certifications like OCA- DBA/OCPDBA/MCDBA	1

6. Instruction to Bidders

CIDCO through the process of e-tendering invites "ONLINE" item rate percentage bid from the reputed perspective firms with experience of similar type of works of Website redesign and development and Cloud infrastructure services for the work mentioned under the Scope of Work section of this document.

6.1. Procedure for Submission of Bids

- To view Tender Notice, Detailed Time Schedule, Tender Document for this Tender and subsequently download the Tender Document and its supporting documents, kindly visit following e-Tendering website: https://mahatenders.gov.in/.
- The Bidders participating first time for e-Tenders on GoM e-tendering website will have to complete the Online Registration Process for the e-Tendering website.
- All Bidders interested in participating in the on-line 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.

6.2. Language of Bid

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

6.3. Bid Submission

- Submission of bids shall be in accordance with the instructions given in the Table below:

Particulars	Instructions
EMD	Online Payment of ₹ 4,00,000/(INR Four Lakhs Only) to be paid via online Payment Gateway mode. The information of E-Payment Gateway available on E-Tendering Website https://mahatenders.gov.in.
Tender Processing Fees	₹ 5,900/- (INR Five Thousand Nine Hundred only including GST) (Non-Refundable)
Mandatory Eligibility Criteria (Pre-qualification Criteria)	The bidder must prepare the proposal in accordance with the requirements specified in the tender document along with the requisite supporting to establish the compliance to the criteria specified under this tender document.
Commercial Proposal	All the proposal including the quotes to be submitted online only.
Note: The front page of the proposal document shall indicate the name and address of the Bidder agency.	

- CIDCO will not accept delivery of Proposal in any manner other than that specified in this tender document. Proposal delivered in any other manner shall be treated as defective, invalid, and rejected.
- If any Bidder does not qualify the mandatory elegibility criteria stated in the tender document, the commercial proposals of the Bidder shall not be opened.
- It is required that all the Bids submitted in response to this tender document, should be unconditional in all respects, failing which CIDCO reserves the right to reject the Bid.
- Late Bid offers: Bidder's grievance / complaint on account of non-submission of Bid due to problem in internet, electricity or any other reason.

6.4. Pre-bid Queries

CIDCO will host a Pre-Bid Meeting for queries (if any) raised by the prospective bidders. The Meeting will be held on //2023. Venue and time of the Meeting will be communicated separately to all the bidders. The representatives of the bidders may attend the pre-bid meeting at their own cost. The purpose of the pre-bid meeting is to provide a forum to the bidders to clarify their doubts / seek clarification or additional information, necessary for them to submit their bid.

All enquiries from the bidders relating to this RFP must be submitted by Email to sm.dc@cidcoindia.com The queries should necessarily be submitted in the following format in an excel document:

Sr. No.	Company Name	Section No.	Page No.	Content of the RFP requiring clarification	Clarification Sought
1 2 …	XXX	5.6	12	<Pre-Bid Queries>	<Clarification>

Queries submitted post the above-mentioned deadline, or which do not adhere to the above-mentioned format may not be responded to.

6.5. Prices and Price Information

The Bidder shall quote a price that are necessary to meet the requirements of the tender document.

- All the prices will be in Indian Rupees only.
- All prices should be rounded off to the nearest Indian Rupees (If the first decimal value is 5 (five) or above it should be rounded up and below 5 (five) should be rounded down.
- The price quoted in the Commercial Proposal shall be the only and maximum payment payable by CIDCO to the successful bidder for completion of the contractual obligations by the successful bidder under the Contract, subject to the terms of payment and performance levels specified in this tender document.
- The Total Contract Value should be inclusive of all costs that required to perform all the contractual obligations under this tender document. No additional cost will be entertained in any manner whatsoever.
- The price would be inclusive of all taxes, duties, charges, and levies as applicable but excluding GST.

- The prices, once offered, must remain fixed and must not be subject to escalation for any reason whatsoever within the period of the Contract. No revision of the Total Contract Value shall be made on account of any variations in costs of labor and materials, currency exchange fluctuations with international currency or any other cost component affecting the total cost in fulfilling the obligations under the Contract. A Proposal submitted with an adjustable price quotation or conditional Proposal may be rejected as non-responsive.
- Bidder should provide all prices, quantities as per the prescribed format given in the Commercial Bid format in the tender document. In case the field is not applicable, Bidder must indicate "0" (zero) in all such fields. In case the Bidder leaves a cell blank, it will be taken as "0" (zero).
- All costs incurred due to delay of any sort attributable to the Bidder, shall be borne by the Bidder.

6.6. Correction of Errors in Commercial Proposal

- Bidders are advised to exercise adequate care in quoting the prices. No excuse for corrections in the quoted figures will be entertained after the Commercial Proposals are received by CIDCO.
- The quoted price shall be corrected for arithmetical errors.
- In cases of discrepancy between the prices quoted in words and in figures, lower of the two shall be considered. The successful bidder is required to execute a contract agreement in the proforma attached with the Bid documents on stamp paper of appropriate value as per Maharashtra Stamp Act, 1958 (as amended from time to time). The contract agreement should be executed within 30 days from the date of receipt of acceptance letter.
- The amount stated in the Commercial Proposal, adjusted in accordance with the above procedure and shall be considered as binding on the Bidder for evaluation.

6.7. Disqualification

The Proposal is liable to be disqualified in the following cases or in case the Bidder fails to meet the bidding requirements as indicated in this tender:

- Proposal not submitted in accordance with the procedure and formats prescribed in this document or treated as non-conforming Proposal.
- During validity of the Proposal, or its extended period, if any, the Bidder increases his quoted prices or withdraws their proposal.
- Proposal is received in incomplete form.
- Proposal is not accompanied by all the requisite documents.
- Proposal is not accompanied by the EMD.
- Information submitted in Proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly, or otherwise, at any time during the processing of the Contract (no matter at what stage) or during the tenure of the Contract including the extension period, if any.
- Commercial quote appeared in any other place other than the place specified.
- Bidder tries to influence the Proposal evaluation process by unlawful / corrupt / fraudulent means at any point of time during the Bid process.

- In case any one Bidder submits multiple Proposals or if common interests are found in two or more Bidders, the Bidders are likely to be disqualified, unless additional Proposals/Bidders are withdrawn upon notice immediately.

6.8. Consortium / Joint Venture

Consortium / Joint Venture is NOT allowed for the purpose of this bid

6.9. Sub-Contracting

Sub-Contracting is not allowed.

7. Bid Opening and Proposal Evaluation Process

- Bid opening will be conducted in two stage.
- The Bid submitted without EMD, will be summarily rejected. Only those Bid for which EMD is received will be eligible for opening.
- Total transparency will be observed and ensured while opening the Proposals/Bids.
- CIDCO reserves the rights at all times to postpone or cancel a scheduled Bid opening.
- In the first stage, Pre-qualification cum Technical Proposals would be opened.
- In the second stage, Commercial Proposal of those Bidders who qualify the mandatory eligibility criteria, would be opened.
- At any time during the tender evaluation process, CIDCO may seek written clarifications from the Bidders. The primary function of clarifications in the evaluation process is to clarify ambiguities and uncertainties arising out of the evaluation of the Bid documents. Written clarifications provide the opportunity for CIDCO to state its requirements clearly and for the Bidder to more clearly state its Proposal. CIDCO may seek inputs from their professional and technical experts in the evaluation process.
- CIDCO reserves the right to do a reference check in all respect stated by the Bidder. Any feedback received during the reference check shall be taken into account during the evaluation process

7.1. Evaluation of Pre-Qualification and Technical Proposal

- Bidders whose EMD and tender document fees are found in order, shall be considered for Pre-Qualification Proposal evaluation.
- Bidder shall be evaluated as per mandatory eligibility criteria mentioned in the tender document. The bidders who fulfil all the criteria will qualify for further technical evaluation.

7.1.1. Mandatory Eligibility Criteria (Pre-qualification Criteria)

The minimum eligibility criteria that should be satisfied by the Bidders are mentioned below. The formats for the Pre-qualification documents are given in the tender document, unless specified otherwise.

#	Basic Requirement	Criterion	Supporting documents to be submitted with the Bid
PQ1	Tender Fees	The bidder should have made a payment of ₹ 5,900/- (INR Five Thousand Nine Hundred only including GST) (Non-Refundable) for the Tender Fees.	Cost of tender document must be submitted through e-payment only.
PQ2	EMD	The bidder should have submitted EMD of ₹ 4,00,000/- (INR Four Lakhs Only) through Online payment gateway available in the e-tendering website. Note: Any request or waiver for EMD exemption will not be entertained.	EMD to be paid via online Payment Gateway mode. The information of E-Payment Gateway available on E-Tendering Website https://mahatenders.gov.in
PQ3	Legal Entity	The Bidder: • Shall be a company registered under the Companies Act, 2013 or the Companies Act, 1956 or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 • Shall be registered with GST Authorities in India • Should have their registered offices with legal presence in Mumbai Metropolitan Region.	The bidder shall submit following documents: ➢ Copy of Certificate of Incorporation/ Registration/ Partnership deed signed by Authorized Signatory of Bidder. ➢ Copy of PAN Card ➢ Copy of GST certificate
PQ4	Financial Strength	The bidder should have an average annual turnover of at least 24 crores for last 3 financial years (FY'20-21, FY'21-22, FY 22-23) from IT/ITeS /Cloud Infrastructure services. Average annual Turnover of the cloud service provider should be at least INR 1000 Crores for last three financial years.	The bidder to submit the- Audited Balance Sheet and Profit & Loss Account Statement of the Bidder for each of the last 3 audited financial years FY'20-21, FY'21-22, FY 22-23 AND • Certificate duly signed by Statutory Auditor/CA of the Bidder for total turnover and turnover from the field of IT/ITeS services /Cloud Infrastructure services.
PQ5	Financial Strength	The bidder should have positive net worth for last three financial years (FY'20-21, FY'21-22, FY 22-23)	The bidder shall submit following document:

#	Basic Requirement	Criterion	Supporting documents to be submitted with the Bid
			• Certificate from the Statutory auditor/ Chartered Accountant clearly specifying the said requirement.
PQ6	Similar Experience	The bidder must have experience in projects related to IT related services involving Design Development, Implementation and Maintenance of an official Website implementation or maintenance of cloud infrastructure service in Govt./Semi. Govt. sectors / PSUs in last 5 years as on bid submission date: At least one (01) project (which includes development & maintenance of web application) of value not less than INR 3.4crore OR At least two (02) projects (which includes development & maintenance of web application), each of value not less than INR 2.5crore OR At least three (03) projects (which includes development & maintenance of web application), each of value not less than INR 1.7crore	The bidder shall submit following documents: • Copy of Work order/ Contract clearly highlighting the scope of work and value of the contract / order. or • Copy of Completion Certificate/ Milestone / Phase Completion Certificate issued & signed by the competent authority of the client's entity on the entity's letterhead/ self-declaration certifying successful execution of project.
PQ7	Authorization	The bidder must be a certified Service Partner of the Cloud Service Provider as per the requirement provided in this tender document. Cloud service provider should have their data centre in India.	MAF (Manufacturer Authorisation Form) to be submitted from Cloud Service Provider in their letter heads.
PQ8	Technical and Functional Compliance	The selected bidder must provide their compliance with the technical and functional requirements with respect to cloud infrastructure	The compliance details as mentioned in **Annexure 9.2** with Certificate issued & signed by the competent authority of the client's entity on the entity's letterhead

#	Basic Requirement	Criterion	Supporting documents to be submitted with the Bid
PQ9	Workforce Strength	The bidder must have on its roll a minimum of 50 qualified IT staff experienced in designing, development, implementation, and maintenance of the official website. In addition, the resources must have relevant experience in projects related to implementation and maintenance of cloud infrastructure services.	The sole bidder shall submit following documents: • Declaration letter from HR on company letter head stating the same.
PQ10	Certification	The bidder should have an ISO 9001:2015, ISO: 27001 certification and should be an SEI CMM Level 3 or above certified organization.	• Copies of the valid certificates from authorized agencies
PQ11	Blacklisting	The bidder should not be debarred /blacklisted by any Government / PSU / Semi- Government Sector in India as on date of submission of the Bid.	The bidder needs to submit a Self-Declaration in the format as provided in this tender document stating that the bidder has not been debarred/ blacklisted by any Government / PSU / Semi-Government Sector in India.
PQ12	Non-Penalization	The bidder should not have been penalized or received a show cause notice from Public Sector Undertakings (PSU) companies/ Urban Local Bodies/ Central Government / State Government Organizations in last five consecutive financial years (FY 18-19,19-20, 20-21,21-22-22-23)	Affidavit on Rs. 500 stamp paper stating that the bidder has not been penalized or received a show cause notice from Public Sector Undertakings (PSU) companies/ Urban Local Bodies/ Central Government / State Government Organizations in last five consecutive financial years (FY 18-19,19-20, 20-21,21-22-22-23)

- Any bid failing to meet all the above eligibility criteria shall be disqualified and will not be considered for technical evaluation.
- Change in eligibility criteria during bidding stage: It is bidder's responsibility to bring any change to CIDCO's notice if there is a change in the status of the bidder during bidding stage, with reference to any of the above-mentioned criteria for eligibility.
- Documentation proof should be submitted as per the formats prescribed above.

7.2. Technical Evaluation Criteria

- Each Technical Proposal will be assigned a Technical Score out of a maximum of 100 points.

- To qualify for the opening of Commercial Proposal, the Bidder must get a minimum overall Technical Score of 70 (Seventy).
- The Commercial Proposals of Bidders who do not qualify technically shall be kept unopened in the e-Tendering system.
- The Committee shall indicate to all the Bidders the results of the Technical Evaluation through a written communication. The Technical Scores of the Bidders will be announced prior to the opening of the Commercial Proposals.
- The technically shortlisted Bidders will be informed of the date and venue of the opening of the Commercial Proposals through email or written communication.
  Technical Evaluation Criteria

Sr No.	Technical Evaluation Parameters	Maximum Marks
1	Bidder's Profile	30
2	Bidder's Similar Work Experience	30
3	Bidders Proposed Key Resources	10
4	Bidders Presentation (Approach & Methodology)	30
	Total	100

<table>
<tr><th>#</th><th>Criteria</th><th colspan="2">Evaluation parameters</th><th>Documents Required</th></tr>
<tr><td colspan="5">I. Bidders Profile (Turnover & Certification) – Maximum 30 Marks</td></tr>
<tr><td rowspan="5">TQ-1</td><td rowspan="5">The bidder should have an average annual turnover of at least Rs. 24 Crore for last 3 financial years (FY'20-21. FY'21-22 & FY 22-23) from IT/ITeS /Cloud Infrastructure services.</td><td>Turnover</td><td>Marks</td><td rowspan="5">The bidder shall submit following documents:
• Audited Balance Sheet and Profit & Loss Account Statements of the Bidder for each of the last 3 audited financial years FY'20-21. FY'21-22 & FY 22-23, audited balance sheet and profit & loss statement certified by Chartered Accountant to be provided.
• Certificate from the statutory auditor/ CA clearly specifying turnover details of the company from "IT/ITES Services" for financial years FY'20-21. FY'21-22 & FY 22-23,</td></tr>
<tr><td>>=24 Cr. to < 35 Cr. Crore</td><td>10</td></tr>
<tr><td>>=35 Cr. to < 50 Cr. Crore</td><td>12</td></tr>
<tr><td>>=50 Cr.</td><td>15</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="3">TQ-2</td><td rowspan="3">The bidder should have an ISO 9001:2015 certification and ISO 27001 certification.</td><td>Certification</td><td>Marks</td><td rowspan="3">The bidder shall submit following documents:
• Valid certificate from the recognized organization</td></tr>
<tr><td>ISO 9001:2015 or ISO 27001 Certification</td><td>3</td></tr>
<tr><td>Both the certification</td><td>5</td></tr>
<tr><td rowspan="3">TQ-3</td><td rowspan="3">The bidder should be an SEI CMMi Level 3 or above certified organization.</td><td>Certification</td><td>Marks</td><td rowspan="3">The bidder shall submit following documents:
• Valid certificate from the recognized organization.</td></tr>
<tr><td>SEI CMMi Level 3</td><td>5</td></tr>
<tr><td>SEI CMMi Level 5</td><td>10</td></tr>
<tr><td colspan="5">II. Experience – Maximum 30 Marks</td></tr>
</table>

<table>
<tr><th>#</th><th>Criteria</th><th colspan="2">Evaluation parameters</th><th>Documents Required</th></tr>
<tr><td rowspan="5">TQ-4</td><td rowspan="5">The bidder must have experience in projects related design / development/ implementation / Maintenance of official website projects/IT/ITes applications and implementation and maintenance of cloud infrastructure service in Govt./Semi. Govt. sectors / PSUs in last 5 years as on bid submission date</td><td>Project Numbers</td><td>Marks (Maximum 30 Marks)</td><td rowspan="5">The selected bidder shall submit following documents:
• Project reference shall be provided in the format prescribed in the RFP and be duly certified by Authorized Signatory.
AND
• Copy of Work order/ Contract clearly highlighting the scope of work and value of the contract / order
AND
• Copy of Completion Certificate/ Milestone / Phase Completion Certificate issued & signed by the competent authority of the client’s entity on the entity’s letterhead/ self-declaration certifying successful execution of project.</td></tr>
<tr><td>>=1 to < =3</td><td>20</td></tr>
<tr><td>>3 to <=6</td><td>25</td></tr>
<tr><td>>6</td><td>30</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="5">III. Key Professionals Profile (CV) – Maximum 10 Marks</td></tr>
<tr><td rowspan="4">TQ-5</td><td rowspan="4">The bidder must have on its roll a minimum of 50 qualified IT staff (across offices) experienced in managing</td><td colspan="2">Number of resources</td><td>Marks</td><td rowspan="4">Copy of undertaking from HR declaring the number of resources with surveillance experience on the company payroll.</td></tr>
<tr><td colspan="2">>=50 and <80</td><td>4</td></tr>
<tr><td colspan="2">>=80 and <100</td><td>6</td></tr>
<tr><td colspan="2">>=100</td><td>10</td></tr>
<tr><td colspan="5">IV. Approach & Methodology – Maximum 30 Marks</td></tr>
</table>

#	Criteria	Evaluation parameters	Documents Required
TQ-6	The bidder needs to present its Approach and Methodology covering the below areas: • Understanding of Scope of work • Transition Management • Project Management methodology for Support & Maintenance • SLA Compliance		-Presentation
Total Technical Evaluation Marks			**100**

- Evaluation shall be done based on the information provided in the technical proposal and clarifications / answers given by the bidders to the queries raised by CIDCO, if any.

7.3. Evaluation of Commercial Proposals

CIDCO will open the Commercial Bids of only the technically qualified department, in the presence of the representatives of the Bidders who choose to attend, at the time, date and place, as decided by the department.

The Commercial Bids will be opened and compared (after the technical evaluation is completed) for those Bidders whose technical bids reach the minimum threshold standards (i.e., 70 marks).

Bidder "Scoring highest as per QCBS Process" will be considered for selection.

7.4. Selection of bidder

- Evaluation criteria proposed to be adopted will be Quality cum Cost Based System (QCBS) where Technical Bid Score will get a weightage of 70% and Commercial Bid Score a weightage of 30%.
- The bidder would be technically evaluated out of 100 marks. All the bidders who secure overall minimum of 70% (70 Marks out of 100 as per technical evaluation criteria) will be considered as technically qualified. Technical score of all bidders will be calculated on the basis of the following formula:

  Technical Score of bidders (TS) = Technical Marks received by the bidder (out of 100)/Technical score of the highest bidder x 70%

- The Bid having the Lowest Commercial Quote shall be termed as the Lowest Evaluated Bid and will be awarded full marks of commercial bid. Commercial score of all the other bidders will be calculated on the basis of the following formula:

  Commercial score of bidders (CS) = (Commercial Quote of the lowest bidder/Commercial Quote of the Concerned Bidder) x 100 x 30%

- Final Total Score of the bidder: Final Score of each bidding party will be computed by adding the technical score and Commercial Score based on the following formula:

  Total Score = TS + CS

- The bidder whose bid has secured the "Highest Total Score" out of 100 as per above evaluation will be considered as best evaluated Bid for selection. In case of a tie where two or more bidders achieve the same highest overall score, the bidder with the higher technical score will be selected.
- After selection, a letter of Award (the "LOA") shall be issued in duplicate by the department to selected bidder and selected bidder shall within seven days of receipt of LOA, sign and return the duplicate copy of LOA in acknowledgement thereof. In the event the duplicate copy of LOA duly signed by selected bidder is not received by the stipulated date, department may, unless it consents to extension of time for submission thereof, appropriate the EMD of such bidder as damages on account of failure of the selected bidder to acknowledge the LOA.
- After acknowledgement of LOA as aforesaid by selected bidder, it shall cause the concessionaire to execute the concession agreement within the period prescribed. The selected bidder shall not be entitled to seek any deviation, modification, or amendment in the concessionaire agreement.

7.5. Award of Contract

Post the evaluation process indicated above, CIDCO will award the Contract to the Bidder whose Proposal has been determined to be technically responsive to the requirements of the tender document and financially the lowest price, hereby referred to as the 'Successful bidder'.

7.6. Right to accept and to reject any Proposal.

CIDCO reserves the right to accept or reject any Proposal, and to annul the tendering process and reject all Proposals at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for CIDCO's action.

7.7. Notification of Award

Prior to the expiration of the validity period, CIDCO will notify the Successful bidder that its Proposal has been accepted by issuance of a Letter of Acceptance in writing or through email. Until a formal contract is prepared and executed, Letter of Acceptance shall constitute a binding Contract.

7.8. Performance Bank Guarantee

A PBG of 3% of the Total Contract Value would be furnished by the successful bidder as per the format provided in the tender document from Nationalized/Scheduled Bank. The PBG should be furnished within 15 Business Days from the date of issue of Letter of Acceptance and should be valid for period of 180 days over and above the Contract Period.

7.9. Signing of Contract

CIDCO shall have the right to annul the award in case there is a delay of more than 30 days in signing of Contract from the date of issue of Letter of Acceptance by CIDCO, for reasons attributable to the successful bidder.

The successful bidder is required to execute a contract agreement in the pro-forma attached with the Bid documents on stamp paper of appropriate value as per Maharashtra Stamp Act, 1958 (as amended from time to time). The contract agreement should be executed within 30 days from the date of receipt of acceptance letter.

CIDCO shall sign the Contract with **successful bidder for a period of 3 years** from the date of issue of work. The contract can be further extended based on performance of the Service Provider and at CIDCO's discretion. During the tenure of the project, if the performance of the selected bidder is not found appropriate then CIDCO at its discretion may terminate the contract at any point of time as per the terms specified in Termination Section of tender document.

Failure to agree with Terms and Conditions of this Tender.

Failure of the successful bidder to agree with the terms & conditions of the tender document shall constitute sufficient grounds for the annulment of the award, in which event CIDCO may call for new Proposals and invoke the Performance Bank Guarantee (PBG).

7.10. General Terms and Conditions

7.10.1. Applicable Law

The Contract shall be interpreted in accordance with the laws of the Union of India.

7.10.2. Taxes and Duties

The service provider shall fully familiarize themselves about the applicable Domestic taxes on amount payable by CIDCO under the contract. The service provider shall pay such domestic tax, duties, fees and other impositions (wherever applicable) levied under the applicable law.

The taxes quoted in the offer should be as per the prevailing tax rates. Any subsequent increase in the tax rates or introduction of new tax will be paid by CIDCO. Similarly, any benefits arising due to downward revision in tax rates, or any exemptions availed by the Bidder organization should be passed on to CIDCO.

7.10.3. Change in Laws and Regulations

Unless otherwise specified in the Contract, if after the date of the Invitation for Bids, any law, regulation, ordinance, order or bylaw having the force of law is enacted, promulgated, abrogated, or changed that subsequently affects the Delivery Date and/or the Contract Price, then such Delivery Date and/or Contract Price shall be correspondingly increased or decreased, to the extent that the successful bidder has thereby been affected in the performance of any of its obligations under the Contract.

7.10.4. Termination

Termination by CIDCO

1. CIDCO may, without prejudice to any other remedy for breach of Contract, terminate this Contract in case of the occurrence of any of the events specified under this clause. In such an occurrence, CIDCO shall give a not less than 30 days' written notice of termination to the successful bidder.
2. If the successful bidder does not remedy a failure in the performance of its obligations under the Contract, within thirty (30) days after being notified or within any further period as CIDCO may have subsequently approved in writing.
3. If the successful bidder becomes insolvent or goes into liquidation, or receivership whether compulsory or voluntary.
4. If the successful bidder, in the judgment of CIDCO has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.
5. If, as the result of Force Majeure, the successful bidder is unable to perform a material portion of the Services for a period of not less than 60 days.
6. If the successful bidder submits to the CIDCO a false statement which has a material effect on the rights, obligations, or interests of CIDCO.
7. If the successful bidder places itself in a position of conflict of interest or fails to disclose promptly any conflict of interest to CIDCO.
8. If the successful bidder fails to provide the quality services as envisaged under this Contract, CIDCO may make judgment regarding the poor quality of services, the reasons for which shall be recorded in writing. CIDCO may decide to give one chance to the successful bidder to improve the quality of the services.

9. If the successful bidder fails to comply with any final decision reached as a result of arbitration proceedings.
10. If CIDCO, in its sole discretion and for any reason whatsoever, decides to terminate this Contract.
11. In the event CIDCO terminates the Contract in whole or in part, pursuant to GTC Clause 7.10.4 , CIDCO may procure, upon such terms and in such manner as it deems appropriate, services similar to those undelivered or not performed, and the successful bidder shall be liable to CIDCO for any additional costs for such similar services. However, the successful bidder shall continue performance of the Contract to the extent not terminated.

7.10.5. Payment upon Termination

Upon termination of this Contract pursuant to GTC Clauses 7.10.4 CIDCO shall make the following payments to the Successful bidder:

- If the Contract is terminated pursuant to GTC Clause 7.10.4 (10), remuneration for Services satisfactorily performed prior to the effective date of termination.
- If the agreement is terminated pursuant of GTC Clause 7.10.4. (1) to (9). The successful bidder shall not be entitled to receive any agreed payments upon termination of the contract. However, the CIDCO may consider making a payment for the part satisfactorily performed on the basis of Quantum Merit as assessed by it if such part is of economic utility to the CIDCO. Applicable under such circumstances, upon termination, the CIDCO may also impose liquidated damages. The successful bidder will be required to pay any such liquidated damages to CIDCO within 30 days of termination date.

7.10.6. Payment Terms

- The payment to the Selected Agency will be done based on the milestones delivered as defined in the payment schedule and for the AMC and cloud services it will be done in equal quarterly payments. The AMC/Cloud services value of the project will be distributed in 12 quarters, and the payment will be made in equal quarterly instalments after adjusting the applicable penalties for the same quarter.
- Quarterly payment shall be calculated on acceptance of invoices submitted by vendor on Quarterly basis along with the monthly preventive maintenance report for that quarter, along with the copy of receipt of all license and royalty fees, airtime fees etc.
- The payment towards the deployment of website and migration will be done post successful migration and implementation. The payment for the same will be processed post implementation clearance based on the successful UAT along with the acknowledgment receipt from user or CIDCO.
- The payment towards the change request to be made on the actuals. The efforts approved by the System Manager will only be considered for the final invoicing and payment. The SLAs as specified in section Service Level Agreement will also be applicable at the time of releasing the payment.

Sr No	Activity	Timeline	Payment
1	Migration of website & Data from existing Service provider	Within 3 weeks from the date of acceptance of LOA.	60% of Migration Charges
2	Mock Drill and Operational Acceptance of website	Within 6 weeks from the date of acceptance of LOA.	40% of Migration Charges
3	Deployment of the revamped upgraded website	Within nine weeks from the date of acceptance of LOA	60% of website revamp cost
4	Website Operational Acceptance and Go Live	Within twelve weeks from the date of acceptance of LOA	40% of website revamp cost
5	Cloud services	Will start from the date of LOA acceptance	Quarterly Payment after completion of each quarter after deduction of penalties if any
6	Operation and Maintenance	Will start from the date of Operational Acceptance and Go live	Quarterly Payment after completion of each quarter after deduction of penalties if any

Note:

- If the Bidder 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 Bidder.
- Payment of first instalment will be released only after the receipt of Performance Bank Guarantee.
- CIDCO will release the payment after 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. CIDCO shall be entitled to delay or withhold the payment of a disputed invoice or part of it delivered by Service Provider, when CIDCO disputes such invoice or part of it, provided that such dispute is bona fide.
- In case Go-Live is delayed, the corresponding operations and maintenance phase will start after the Go-Live has been completed.
- AMC and Cloud services Payment will be made quarterly. Payment for subsequent quarters will be made only after payment of previous quarters has been released.
- Payment will be released as per actual utilization of resources. No payment for unutilized resources will be released by CIDCO.
- 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 Rupees as specified in the Commercial Bids.

CIDCO will release the payment within 30 days of submission of valid invoice along with all the supporting, subject to the condition that invoice and all supporting documents produced are in order and work is performed to the satisfaction of CIDCO.

8. Service Level Agreement

8.1. Purpose

The purpose of Service Levels is to define the levels of service provided by the Successful Bidder to CIDCO ("Client") for the duration of the contract. The benefits of this are:

- Help the Client control the levels and performance of service provider's services.
- Create clear requirements for measurement of the performance of the system and help in monitoring the same during **the** Contract duration.

The Service Levels are between the Client and Service Provider

8.1.1. Principles of Service Level Agreements

Service Level Agreement (SLA) shall become the part of the Contract between the Client and the Successful Bidder. SLA defines the terms of successful bidder's responsibility in ensuring the timely delivery of the services and the correctness of the services based on the agreed performance indicators as detailed in this section.

The successful bidder shall comply with the SLAs to ensure adherence to project quality and availability of services throughout the duration of the Contract. For the purpose of the SLA, definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:

- Response time is the time interval between a cloud service customer-initiated event (e.g., logging of the request) and a cloud service provider-initiated event in response to that stimulus.
- Scheduled Maintenance Time shall mean the time that the System is not in service due to a scheduled activity. Scheduled maintenance time is planned downtime with the prior permission of CIDCO, during non-business hours. The Scheduled Maintenance time as agreed shall not be considered for SLA Calculation.
- Scheduled operation time means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time.
- Availability means the time for which the cloud services and facilities are available for conducting operations on CIDCO system. Availability is defined as:
  {(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} * 100%
- Incident refers to any event/issue that affects the normal functioning of the services / infrastructure, reported by the cloud consumer to the Service provider (successful bidder) can be termed as an Incident.
- "Resolution Time" – Time elapsed from the moment incident is reported to the Helpdesk either manually or automatically through system, to the time by which the incident is resolved completely and services as per the Contract are restored.
- Maximum Data Restoration Time: refers to the committed time taken to restore cloud service customer data from a backup.
- Recovery Point Objective: It is the maximum allowable time between recovery points. RPO does not specify the amount of acceptable data loss, only the acceptable time window. RPO affects data redundancy and backup.
- Recovery Time Objective: It is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences. Cloud services can be critical components of business processes.

8.1.2. Service Level Monitoring

- The Service Level parameters shall be monitored on a quarterly basis. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of CIDCO or an agency designated by them, then CIDCO will have the right to take appropriate disciplinary actions including termination of the contract.
- The full set of service level reports should be available to CIDCO on a monthly basis or based on the project requirements.
- Penalties associated with performance for SLAs shall be made after deducting from applicable payments of the quarter or through the Performance Bank Guarantee.
- As part of the Project requirements, successful bidder shall supply and make sure of appropriate system (software/hardware) to automate the procedure of monitoring SLAs during the course of the Contract and submit reports for all SLAs as mentioned in this section. This software along with any system specific software shall be used by the successful bidder for monitoring and reporting these SLAs. The Client reserves the right to test and audit these tools for accuracy and reliability at any time. If at any time during the test and audit the accuracy and reliability of tools shall be found to be compromised, the Client reserves the right to invoke up to double the penalty of the respective quarterly phase.
- In case of default on any of the service level metric, the successful bidder shall submit performance improvement plan along with the root cause analysis for CIDCO's approval.
- Successful bidder undertakes to notify the Client of any difficulties, or detrimental/adverse findings as soon as possible once they are identified.
- Successful bidder will provide a supplemental report on any further information received, as soon as the information becomes available.
- In case issues are not rectified to the complete satisfaction of Client, within a reasonable period of time defined in the RFP, the Client shall have the right to take appropriate remedial actions including liquidated damages, applicable penalties, or termination of the Contract.
- For issues i.e., breach of SLAs beyond control of the Successful bidder, the Successful bidder shall submit a justification for the consideration of the Client. In case it is established that the SP was responsible for such breach, respective penalty shall be applied to the Successful bidder.

8.1.3. Penalties

- The payment should be linked to the compliance with the SLA metrics.
- The penalty in percentage of the Quarterly Payment is indicated against each SLA parameter in the table.
  - For ex: For SLA1 if the penalty to be levied is 7% then 7% of the Quarterly Payment is deducted from the total of the Quarterly bill and the balance paid to the Successful bidder.
  - If the penalties are to be levied in more than one SLAs, then the total applicable penalties are calculated and deducted from the total of the Quarterly bill and the balance paid to the SP.
  - For ex: SLA1 =7% of the Quarterly Payment, SLA2=10% of the Quarterly Payment, SLA3=2% of the Quarterly Payment then
  - Amount to be paid = Total Quarterly bill – {(19% of the Quarterly Payment)}
- In case multiple SLA violations occur due to the same root cause or incident then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a sum of penalties for the applicable SLA violations.
- Penalties shall not exceed 100% of the Quarterly bill. If the penalties exceed more than 50% of the total Quarterly bill, it will result in a material breach. In case of a material breach, the operator will be

given a cure period of one month to rectify the breach failing which a notice to terminate may be issued by the user CIDCO.

8.1.4. Service Levels

The following SLAs apply both for service provider for cloud infrastructure and web redesign and development. The service provider will be responsible for maintaining the SLAs pertaining to the cloud infrastructure, network, controls, managing and monitoring the cloud service and website redesign and development.

8.1.5. Cloud Services

#Sno	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty
Availability/Uptime				
1	Availability/Uptime of cloud services Resources for Production environment (VMs, Storage, OS, VLB, Security Components,)	Availability (as per the definition in the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud.	Availability for each of the provisioned resources: >=99.7%	Default on any one or more of the provisioned resources will attract penalty as indicated below. <99.7% - >=99% (10% of the Quarterly Payment) < 99% (20% of the Quarterly Payment)
2	Availability of Critical Services (e.g., Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / Deactivation; User Profile Management; Access Utilization Monitoring Reports) over User / Admin Portal and APIs (where applicable)	Availability (as per the definition in the SLA) will be measured for each of the critical services over both the User / Admin Portal and APIs (where applicable)	Availability for each of the critical services over both the User / Admin Portal and APIs (where applicable) >= 99.7%	Default on any one or more of the services on either of the portal or APIs will attract penalty as indicated below. <99.7% - >=99% (10% of the Quarterly payment) < 99% (20% of the Quarterly Payment)

#Sno	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty
3	Availability of the network links at DC and DR (links at DC / DRC, DCDRC link)	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud.	Availability for each of the network links: >= 99.7%	Default on any one or more of the provisioned network links will attract penalty as indicated below. <99.7% - >=99% (10% of the Quarterly Payment) < 99% (30% of the Quarterly Payment)
4	Availability of Regular Reports (e.g., Audit, Certifications,) indicating the compliance to the Provisional Empanelment Requirements.		15 working days from the end of the quarter. If STQC issues a certificate based on the audit, then this SLA is not required.	5% of Quarterly Payment
Support Channels - Incident and Helpdesk				
5	Response Time	Incident management tool for ticket generation must be deployed by the Bidder. Bidder should ensure submission of monthly system generated reports from the incident management tool. 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.	95% within 15minutes	<95% & >=90% (5% of the Quarterly Payment) < 90% & >= 85% (7% of the Quarterly Payment) < 85% & >= 80% (9% of the Quarterly Payment)

#Sno	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty
6	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging. Incident management tool for ticket generation must be deployed by the Bidder. Bidder should ensure submission of monthly system generated reports from the incident management tool	For Severity 1, 98% of the incidents should be resolved within 1 Hour of problem reporting	<98% & >=90% (5% of the Quarterly Payment) < 90% & >= 85% (10% of the Quarterly Payment) < 85% & >= 80% (20% of the Quarterly Payment)
7	Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging must be deployed by the Bidder. Incident management tool for ticket generation. Bidder should ensure submission of monthly system generated reports from the incident management tool	95% of Severity 2 within 4 hours of problem reporting & 95% of Severity 3 within 16 hours of problem reporting	<95% & >=90% (2% of the Quarterly Payment) < 90% & >= 85% (4% of the Quarterly Payment) < 85% & >= 80% (6% of the Quarterly Payment)
Security Incident and Management Reporting				
8	Percentage of timely incident report	Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e.,	95% within 1 hour	<95% & >=90% (5% of the Quarterly Payment) < 90% & >= 85% (10% of the Quarterly Payment) < 85% & >= 80% (20% of the Quarterly Payment)

#Sno	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty
		month). Incident Response - successful bidder shall assess and acknowledge the defined incidents within 1 hour after discovery.		
9	Percentage of timely incident resolutions	Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (month) over the total number of defined incidents to the cloud service within a predefined period. (Month). Measured from Incident Reports	95% to be resolved within 1 hour	<95% & >=90% (5% of the Quarterly Payment) < 90% & >= 85% (10% of the Quarterly Payment) < 85% & >= 80% (20% of the Quarterly Payment)
Vulnerability Management				
10	Percentage of timely vulnerability corrections	The number of vulnerability corrections performed by the cloud service provider - Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e., month, week, year, etc.). • High Severity Vulnerabilities – 30 days - Maintain 99.95% service level	99.95%	>=99% & <99.95% (5% of the Quarterly Payment) >=10% & <99% (20% of the Quarterly Payment) <98% (20% of the Quarterly Payment)

#Sno	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty
		• Medium Severity Vulnerabilities – 90 days - Maintain 99.95% service level		
11	Percentage of timely vulnerability reports	Measured as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e., month, week, year, etc.).	99.95%	>=99% & <99.95% (5% of the Quarterly Payment) >=98% & <99% (10% of the Quarterly Payment) <98% (20% of the Quarterly Payment)
12	Security breach including Data Theft/Loss/Corruption	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected INR 5 Lakhs. This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, CIDCO reserves the right to terminate the contract
13	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time		(e.g., 3 working days from the end of the month)	5% of Quarterly Payment

#Sno	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty
14	Recovery Time Objective (RTO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	<= 45 mins	10% of Quarterly Payment per every additional 2 (two) hours of downtime
15	Recovery Point Objective (RPO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	<= 90 mins	10% of Quarterly Payment per every additional 2 (two) hours of downtime
16	Availability of Root Cause Analysis (RCA) reports for Severity 1 & 2		Average within 5 Working days	5% of Quarterly Payment
Website uptime and webpage loading				
17	Website design and layout finalisation	Successful bidder should present three different layout themes to CIDCO. Three layout themes should be distinctly different from each other. For e.g., in Colour, placement of tabs, visual representation, User accessibility etc. CIDCO shall then select the theme and will give go-ahead for the web application development		
18	Website Uptime (Cloud LAN)	System and Network Monitoring tool to be deployed by the bidder. Application Downtime shall be measured from the time the website becomes unavailable (due to any reasons	<97.0%	10% of Quarterly Payment

#Sno	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty
		whatsoever attributable to the Bidder) till the time it becomes fully available for the above requirements.		
19	Time to load a webpage (Cloud LAN)	System and Network Monitoring tool to be deployed by bidder to measure website response Monthly average from the output generated from the system and network monitoring tool to be considered for measuring SLA compliance.	<=4 seconds 5-8 seconds >8 seconds	No penalty 10% of Quarterly Payment 20% of Quarterly Payment
Onsite deployment of resources				
19	Onsite deployment of resources	The resources should be deployed from the project initiation	Resources deployed as per requirements stated in the RFP	Payment will be only made for resources deployed as per requirement stated in the RFP
20	Absence/Leave from the project	The resources need to be present onsite on all working days of the month.	All employees can take 2 days of leave in a month. However, the same needs to be intimated well in advance to CIDCO. Any leave beyond 2 days to be intimated and approved by CIDCO. Service provider must ensure the replacement also to be provided for	Penalty of 5% per resource In case, the resource is absconding from the onsite project deployment, payment of the same will be withheld from immediate effect.

#Sno	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty
			the interim period.	

Severity Level:

Below severity definition provide scenarios for incidents severity.

Severity Level	Description	Example
Severity 1	Environment is down or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available	Non-availability of VM. No access to Storage, software, or application or any incident by which cloud infra is not available from successful bidder. No availability of website No access to CIDCO applications
Severity 2	Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.	Intermittent network connectivity
Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.	Slowness in accessing the website and applications hosted on cloud

8.1.6. SLA Review Process

During the contract period, it is envisaged that there could be changes to the SLA, in terms of measurement methodology / logic / criteria, addition, alteration or deletion of certain parameters, based on mutual consent of both the parties, i.e., CIDCO and the service provider.

CIDCO and the service provider shall each ensure that the range of the Services under the SLA shall not be varied, reduced or increased except by the prior written agreement of CIDCO and the service provider in accordance with the Change Control Schedule.

The SLAs may be reviewed on an annual basis by CIDCO in consultation with the service provider and

other agencies.

8.1.7. Additional Terms

- The service provider should submit the proofs in case of any outage along with analysis of the root cause of the outage to CIDCO.
- It is the right of CIDCO to bring/deploy any external resources / agencies at any time for SLA review.
- The service provider shall deploy sufficient manpower suitably qualified and experienced in shifts to meet the SLA. The service provider shall appoint as many team members as deemed fit by them, to meet the time Schedule and SLA requirements.

9. Annexures

9.1. Bid Submission Forms and Formats

9.1.1. Format for Pre-Qualification Criteria

Checklist for the documents to be included in the Pre-Qualification Envelope

#	Basic Requirement	Criterion	Supporting documents to be submitted with the Bid
•	Tender Fees	The bidder should have made a payment of ₹ 5,900/- (INR Five Thousand Nine Hundred only including GST) (Non-Refundable) for the Tender Fees.	Cost of tender document must be submitted through e-payment only.
•	EMD	The bidder should have submitted EMD of ₹4,00,000/- (INR Four Lakhs Only) through Online payment gateway available in the e-tendering website. Note: Any request or waiver for EMD exemption will not be entertained.	EMD to be paid via online Payment Gateway mode. The information of E-Payment Gateway available on E-Tendering Website https://mahatenders.gov.in
•	Legal Entity	The Bidder: • Shall be a company registered under the Companies Act, 2013 or the Companies Act, 1956 or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 • Shall be registered with GST Authorities in India • Should have their registered offices with legal presence in Mumbai Metropolitan Region.	The bidder shall submit following documents: • Copy of Certificate of Incorporation/ Registration/ Partnership deed signed by Authorized Signatory of Bidder • Copy of PAN Card • Copy of GST certificate
•	Financial Strength	The bidder should have an average annual turnover of at least 24 crores for last 3 financial years (FY' 20-21 , FY'21-22, FY'22-23) from IT/ITeS /Cloud Infrastructure services. Average annual turnover of the cloud service provider should be at least INR 1000 Crores for last three financial years.	• The bidder to submit the-Audited Balance Sheet and Profit & Loss Account Statement of the Bidder for each of the last 3 audited financial years FY' 20-21 , FY'21-22, FY'22-23. AND

#	Basic Requirement	Criterion	Supporting documents to be submitted with the Bid
•	Financial Strength	The bidder should have positive net worth for last three financial years (FY 20-21, FY 21-22, FY 22-23)	The bidder shall submit following document: • Certificate from the Statutory auditor/ Chartered Accountant clearly specifying the said requirement.
•	Similar Experience	The bidder must have experience in projects related to IT related services involving Design Development, Implementation and Maintenance of an official Website implementation and maintenance of cloud infrastructure service in Govt./Semi. Govt. sectors / PSUs in last 5 years as on bid submission date: At least one (01) project of value not less than INR 3.4crore OR At least two (02) projects, each of value not less than INR 2.5crore OR At least three (03) projects, each of value not less than INR 1.7crore	The bidder shall submit following documents: • Copy of Work order/ Contract clearly highlighting the scope of work and value of the contract / order. AND • Copy of Completion Certificate/ Milestone / Phase Completion Certificate issued & signed by the competent authority of the client's entity on the entity's letterhead/ self-declaration certifying successful execution of project.
•	Authorization	The bidder must be a certified Service Partner of the Cloud Service Provider as per the specification provided in this tender document.	MAF (Manufacturer Authorisation Form) to be submitted from Cloud Service Provider in their letter heads.
•	Technical and Functional Compliance	The selected bidder must provide their compliance with the technical and functional requirements with respect to cloud infrastructure	The compliance details as mentioned in Annexure 9.2 with Certificate issued & signed by the competent authority of the client's entity on the entity's letterhead
•	Workforce Strength	The bidder must have on its roll a minimum of 50 qualified IT staff experienced in designing, development,	The selected bidder shall submit following documents:

#	Basic Requirement	Criterion	Supporting documents to be submitted with the Bid
		implementation, and maintenance of the official website. In addition, the resources must have relevant experience in projects related to implementation and maintenance of cloud infrastructure services.	• Declaration letter from HR on company letter head stating the same.
•	Certification	The bidder should have an ISO 9001:2015, ISO: 27001 certification and should be an SEI CMM Level 3 or above certified organization. The bidder should have STQC audited cloud certification	• Copies of the valid certificates from authorized agencies
•	Blacklisting	The bidder should not be debarred /blacklisted by any Government / PSU / Semi- Government Sector in India as on date of submission of the Bid.	The bidder needs to submit a Self-Declaration in the format as provided in this tender document stating that the bidder has not been debarred/ blacklisted by any Government / PSU / Semi-Government Sector in India.
•	Non-Penalization	The bidder should not have been penalized or received a show cause notice from Public Sector Undertakings (PSU) companies/ Urban Local Bodies/ Central Government / State Government Organizations in last five consecutive financial years (FY 18-19,19-20, 20-21,21-22-22-23)	Affidavit on Rs. 500 stamp paper stating that the bidder has not been penalized or received a show cause notice from Public Sector Undertakings (PSU) companies/ Urban Local Bodies/ Central Government / State Government Organizations in last five consecutive financial years (FY 18-19,19-20, 20-21,21-22-22-23)

9.2. Successful bidder's Technical and Functional Compliance

9.2.1 Cloud Portal Service Provisioning

Sr. No.	Description	Compliance Y/N
1	The Service provider should offer cloud service provisioning portal for to provision cloud services either via portal, mobile app or automated using API.	
2	Cloud service provider should enable to provision / change cloud resources through self service provisioning portal.	
3	Service provider should enable to provision / change cloud resources from application programming interface (API).	
4	The user admin portal should be accessible via secure method using SSL certificate.	
5	Should be able to take snapshot of virtual machines from provisioning portal.	
6	Should be able to size virtual machine and select require operating system when provisioning any virtual machines.	
7	Should be able to predict his billing of resources before provisioning any cloud resources.	
8	CIDCO should be able to set threshold of cloud resources of all types of scalabilities.	
9	Should be able to provision all additional storages required for cloud services.	
10	Should be able to provision any kind of resources either static or elastic resources.	
11	Should get list of all cloud resources from provisioning portal.	
12	Should be able to set minimum and maximum number of virtual machines which will be automatically provisioned as part of horizontal scaling to handle spike in load.	

9.2.2 Cloud Portal

Sr.	Cloud Capabilities	Compliance(Y/N)
1	In order to increase the service availability, the cloud service provider must offer multidimensional scaling of cloud services on the request of CIDCO. Resources like RAM and CPU shall scale vertically as well systems should scale horizontally	
2	Cloud service should enable to provision cloud resources through self service provisioning interface.	
3	Cloud System should enable to provision cloud resources from application programming interface (API)	
4	Cloud System should be accessible via VPN using SSL certificate.	
5	Should be able to create, delete, shutdown, reboot virtual machines from Cloud portal.	
6	Should be able to size virtual machine and select require operating system when provisioning any virtual machines	
7	Should be able to predict billing of resources before provisioning any cloud resources if integrated with billing system.	
8	Should be able to set threshold of cloud resources of all types of scalabilities.	
9	Should be able to provision any kind of resources either static or elastic resources.	
10	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.	
11	The Cloud System shall be capable of allowing applications to self-service compute, network and storage infrastructures automatically but limiting to, based on workload demand.	
12	Should ensure that the virtual machine format is compatible with other cloud systems.	
13	Cloud System should give provision to import cloud VM template from other cloud systems.	
14	Cloud System should support provisioning from self-Cloud Orchestration System to add more storage as and when require by VM.	
15	Cloud System should give provision to attached new block disk to any cloud VM from self-service portal.	
16	The Solution should provide a simple to use intuitive web end experience for Cloud Administrator and User of CIDCO.	
17	The Solution should provide Unified Infrastructure management with complete inventory management of virtual machines & physical resources.	
18	The Solution should provide comprehensive service catalog with capabilities for service design and lifecycle management, a web-based self-service portal for users to order and manage services.	
19	Cloud System should have provision to ensure that cloud virtual machine is into separate network tenant and virtual LAN.	

Sr.	Cloud Capabilities	Compliance(Y/N)
20	Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM	
21	Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM.	
22	Cloud System must ensure the ability to map private IP address of cloud VM to public IP address as require from portal of Cloud Orchestration System.	
23	Should ensure that cloud VM network is IPV6 compatible.	
24	Should support use of appropriate load balancers for network request distribution across multiple cloud VMs.	
25	Cloud Orchestration System should provide network information of cloud virtual resources.	
26	Cloud Orchestration System should have built-in user-level controls and administrator logs for transparency and audit control	
27	Cloud System should support policy-based provisioning of virtual machines. Based on granted permission, users should be able to perform the operations. For example, if any users don't have permission to delete VM, he should not be able to do it.	
28	Cloud System should support quota-based system. Users should not be able to provision resources beyond allocated quota.	
29	The Admin should be able to define Access Control to Permit or Deny operation per Group or per User.	
30	Should have provision to define Workflow to Escalate Permission to Group Admins or System Admins.	
31	The Solution should allow for implementing workflows for provisioning, deployment, Decommissioning all virtual and physical assets in the cloud data center.	
32	User Management: The solution shall provide comprehensive user management	
33	Functions including tenant-specific user grouping and admin/user rights within the scope of a tenant. The tenant-admin user is considered distinct from the overall cloud solution administrator. The tenant-admin shall be able to manage own profile, tenant preferences, as well as users within the tenant/group scope. Individual users shall be able to manage their own profile and individual preferences. The solution administrator shall have the rights to all User Management functions.	
34	Cloud System should provide facility to make template from virtual machines.	
35	Cloud System should give provision to make clone of cloud virtual machine from Cloud Orchestration System.	
36	Cloud System should have provision to live migration of virtual machine to another physical servers in case of any failure.	
37	Cloud System should have provision to migration of virtual machine from one hypervisor platform to another hypervisor platform through its UI.	

Sr.	Cloud Capabilities	Compliance(Y/N)
38	Cloud System cloud shall continuously monitor utilization across Virtual Machines and shall intelligently allocate available resources among the Virtual Machines.	
39	The Cloud System solution shall be able to dynamically allocate and balance computing capacity across collections of hardware resources of one physical box aggregated into one unified resource pool.	
40	The Cloud System cloud solution should support detecting, in real time, resource requirements of a system in virtual environment and automatic scaling of resource parameters like RAM and CPU to compensate resource requirement in a system.	
41	The solution shall provide near zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.	
42	Cloud System should give provision to monitor the network traffic of cloud virtual machine.	
43	Cloud System should offer provision to analyze of amount of data transferred of each cloud virtual machine.	
44	Cloud System must offer provision to monitor uptime of each cloud virtual machine.	
45	Cloud System must make provision of resource utilization graph i.e., RAM 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.	
46	Cloud System must make provision of resource utilization i.e., CPU graphs of each cloud virtual machine.	
47	Cloud System 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.	
48	Cloud System must give provision to monitor the load of Linux/Windows servers and set threshold for alerts.	
49	Cloud System must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.	
50	Cloud System must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity	
51	Should be able to create virtual instances of required configuration without limiting to any standard templates	

9.2.3 General Cloud Requirement

#	Description	Compliance(Y/N)
1	The datacenter shall be at least an Uptime/TIA 942 certified Tier III datacenter providing 99.7% services availability SLAs	
2	The datacenter shall be well equipped with physical, logical, network and infrastructure security solutions, access protection systems including physical access control, and shall maintain the logs of the access.	
3	The datacenter shall be well equipped with intrusion detection & protection systems, firewalls, system management solutions & tools, back-up & restore solutions, monitoring tools, network load balancer for applicable servers and network layer security to isolate CIDCO Web, App and DB environment	
4	The datacenter shall have ability to scale up or down the servers/compute resources on-demand/ as desired without significant down time.	
5	The compute infrastructure shall include the physical / virtual machines, operating systems, application servers, database server, anti-virus solutions and system management & back-up agents.	
6	The IT infrastructure should be hosted on Government Community Cloud.	
7	All the virtual machines should be auto scalable in terms of RAM. and CPU.	
8	The cloud platform should be enough intelligent to predict incoming load and assign resources to virtual machines dynamically without rebooting system.	
9	Cloud platform should always allocate minimum 50% buffer resources against running load to handle sudden spikes.	
10	The cloud platform should provide high availability across virtual machines so that even if any host goes down, all guest virtual machines should be migrated to another host automatically.	
11	Cloud platform should support horizontal load balancing along with vertical. Load balancer should be used to load balance traffic. Load balancer should be able to trigger new virtual machines to handle additional load. If load goes down, newly triggered virtual machines should be recycled.	
12	Cloud provider should give CIDCO a dashboard of all virtual machines to monitor allocated and used resources by APPLICATION and associated applications.	
13	Cloud dashboard should allow to generate reports for trend analysis of system usage.	

#	Description	Compliance(Y/N)
14	CIDCO team should be able to get the console access of any virtual machines if require.	
15	There should be provision to generate historical reports of resources utilization.	
16	There should be admin panel to create, delete, start, stop, and copy virtual machines.	
17	There must be provision to create golden image of virtual machine so that it can be used to make more machines of same configuration	
18	There should be provision to take snapshots of machines so that working images of testing/quality machines can be taken.	
19	successful bidder should provide a VPN solution to the enable CIDCO field offices to access CIDCO applications hosted on cloud in a secure manner. The solution should	
20	successful bidder should procure the service from the any of the service providers and charge a fixed rate to CIDCO during the tenure of the contract. The successful bidder must use the current SMS headers used by CIDCO	

9.2.4 Web Application Firewall (WAF)

#	Description	Compliance (Y/N)
1	Cloud platform should provide Web Application Filter for OWASP (Open Web Application Security Project) Top 10 protection	
2	Service provider WAF should be able to support multiple website security.	
3	Service provider WAF should be able to perform packet inspection on every request covering all 7 layers.	
4	Service provider WAF should be able to block invalidated requests.	
5	Service provider WAF should be able to block attacks before it is posted to website.	
6	Service provider 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	Service provider must offer provision to customize response of vulnerable requests.	
9	Service provider WAF should be able to monitor attack incidents and simultaneously control the attacker IP.	
10	Service provider WAF should be able to Whitelist or Backlist IP/Subnet.	
11	Service provider 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 / block the IP if the threshold is violated.	
13	WAF should be able to set a limit to maximum file size, combined file size in bytes	
14	WAF should be able to limit allowed HTTP versions, request content type, restricted extensions & headers	
15	Service provider WAF should be able to limit maximum number of arguments, argument name, value, value total length etc.	
16	Should be able to BAN an IP for a customizable specified amount of time if the HTTP request is too large.	
17	Should be able to limit maximum size of request body entity in bytes	
18	The WAF should be able to close all the sessions of an IP if it is ban.	
19	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.	
20	The WAF access and security Dashboard should show a graphical representation of	

#	Description	Compliance (Y/N)
	A) For access report analysis purpose, the Dashboard should contain following information:	
	i) Number of hits by status code	
	ii) HTTP status code wise hits	
	iii) HTTP methods wise hits	
	iv) Client browser wise hits	
	v) Client Operating system wise hits	
	vi)Traffic (No. of hits) per URL	
	vii) Average bytes received per request	
	viii) Average bytes sent per request	
	ix) Average time elapsed per request	
	B) For security report analysis purpose, the Dashboard should contain following information:	
	i) Average score by status code	
	ii) Distribution of blocked requests	
	iii) Number of blocked requests	
	iv) OWASP Top 10 requests	
	v) Reputation tags	
	vi) IP list reputation	
	C) For network incoming and outgoing traffic captured by WAF packet filter dashboard should contain following information:	
	i) Number of packet hits	
	ii) Source IP, Destination IP wise hits	
	iii) Firewall actions (allow, deny) wise hits	
	iv) Requests per destination port wise hits	
	D) Geo map of number of hits by country	
21	WAF should support different policies for different web applications.	
22	Vendor to ensure 24x7x365 availability of WAF service.	
23	WAF should support different policies for different application section (different security zones within the app).	
24	WAF should support IP Reputation DB (DB including blacklisted IP Address, IP Address, Anonymous Proxy, Botnets, Windows Exploit etc.) along with Client Source IP address-based Security Policy and dynamic source IP blocking.	
25	WAF should enforce file upload control based on file type, size etc.	
26	WAF should detect known malicious users who are often responsible for automated and botnet attacks. Malicious users may include malicious IP addresses or anonymous proxy addresses.	

#	Description	Compliance (Y/N)
27	WAF should support detection only, blocking and transparent mode.	
28	WAF solution should be capable of handling IPV4 and IPV6 traffic.	
29	WAF solution should ensure compliance and advanced protection against industry standards such as OWASP Top 10 vulnerabilities etc.	
30	Vendor must monitor, manage & maintain the WAF solution on a 24x7 basis.	
31	WAF should provide a real-time dashboard with data such as top attacks view, traffic monitoring view, etc.	
32	WAF should provide role-based access control for the dashboard (role based multiple login accounts both primary and secondary to be provided).	
33	WAF should provide detailed reports for all web application attacks.	
34	WAF should be able to decrypt the SSL traffic to analyze the HTTP data and should be able to re-encrypt the SSL traffic.	
35	WAF should support SSL offloading.	
36	WAF should support body inspection, content injection, backend compression, validation of UTF8 Encoding, XML Inspection.	
37	WAF should block invalid BODY.	
38	WAF should log all transactions for auditing purpose.	
39	WAF should block desktop users User-Agent, crawlers User-Agent, suspicious User-Agent.	
40	WAF should have customizable scoring policy for each request and can block request if global score exceeds.	
41	WAF should have DOS and BF protection for all or specific URLs.	
42	WAF should have learning mode to create whitelist/blacklist rules and also block attack in learning mode.	
43	WAF should verify SSL certificate, certificate name, expiration and cipher suites. Also control over accepted TLS/SSL protocol, cipher order, CRL verification, HTTP public key pinning, OSI stapling.	
44	WAF should allow to inject Request and Response headers for applications.	
45	WAF should support Content and URL rewriting policies.	
46	WAF should send proxy HTTP headers to backend, r rewrite cookie path, backend' s cookies encryption and override backend server HTTP errors.	
47	WAF should support force HTTP to HTTPS redirection.	
48	WAF should have OS level firewall to PASS/BLOCK traffic inbound/outbound traffic	
49	WAF should allow to create custom rules for application.	
50	WAF should support Active-Active/Active-Passive failover.	

9.2.5 Vulnerability Assessment and Monitoring Service

#	Description	Compliance Y/N
1	Monitoring of Web Applications including the corporate websites etc. and protect it from malicious mobile codes like computer viruses, worms, Trojan horses, spyware, adware, key-loggers and other malicious programs. The service should be non-Intrusive in nature.	
2	Malware Monitoring scanning should be performed on Daily basis. If any malware is injected into Web Applications, then immediate malware alert message is forwarded to the stakeholders. Application Audit and Vulnerability assessment on weekly basis to ascertain if any corrective action needs to be taken in application based on any observations found in the scanning.	
3	Should be able to detect malicious code injection/links, both known and unknown malware, Web-page tampering, various zero-day browser exploits etc.	
4	Should be able to identify the malware source, malware threat area and coverage, encoded Java Script and VB script and should not rely on pattern/signature-based technology.	
5	It should have minimal impact on traffic, server performance, networks etc. during deployment and operation	
6	Should be able to work in any network topology.	
7	Should be able to identify applications running on non-standard ports	
8	Should have configurable scan intervals (frequency), Configurable notification, alerting and reporting options, Configurable “whitelist” option for allowed links, Configurable scan schedules and on-demand scans.	
9	Should have Real-time instant alerting upon detection of malicious behavior (Email or SMS).	
10	Should have detailed remediation recommendation guidance including step by step instructions on how to address the threats captured.	
11	Should have On demand Vulnerability Scanning without user intervention	
12	Should Perform a targeted scan (i.e., check for a specific set of vulnerabilities or IP Addresses).	
13	Should be able to conduct vulnerability assessment for all operating systems and their versions including but not limited to: Windows, AIX, UNIX, Linux, Solaris servers etc.	
14	Should be able to perform authenticated and unauthenticated scans	
15	Should be able to detect weak password.	
16	Should be able to identify out-of-date software versions, applicable patches and system upgrades	
17	Should Flag the presence of any blacklisted software	
18	Should be able to perform On demand Application Audit for all types of websites including AJAX, WEB2.0, and obfuscated Java Script etc. and identifies vulnerabilities throughout the entire application, scanning the browser and server-side components.	

#	Description	Compliance Y/N
19	Should check regularly for Defacement Detection, websites change and detect for possible defacement. Such daily defacement checks protect the brand, credibility and reputation of the bank.	
20	Should have an Executive Dashboard that provides a comprehensive synopsis of reported vulnerabilities and malware, remediation suggestions as well as several alert and support options in predefined report formats. It should have Role based access.	
21	Should be able to provide remediation information in the reports including links to patches etc.	
22	Should be able to produce a report listing all applications on a host or network, regardless of whether the application is vulnerable	
23	Should Include a library of potential vulnerabilities and rules which covers SANS (SANS Institute) top 20. This library should be customizable by administrator and changes to the same are to be traceable.	
24	Provide detailed report as spreadsheet, PDF and HTML format, customizable as per the requirement and comparable to previous assessment.	
25	Should be able to generate reports on trends in vulnerabilities on a particular asset.	
26	Should have Scan history and comparison provided in Scan Report.	
27	Should have banner grabbing feature which tries to discover web-applications in the domain.	
28	Should Support industry standard reporting including OWASP top 10 categories.	
29	Should support authenticated scanning with different authentication methods including	
	Form, HTTP basic, NTLM and digest.	
30	The web application vulnerability scanning module should be able to identify the following vulnerabilities but not limited to in the underlying application.	
	· XSS	
	· Form Validation	
	· Block Malformed content	
	· Back Doors	
	· Spoofing	
	· SQL injection	
	· Directory/path traversal	
	· Forceful browsing	
	· LDAP injection	
	· SSID injections	

#	Description	Compliance Y/N
	· XPath injection	
	· Sensitive information leakage	
31	Should be able to check mail server IP and check in multiple RBL repositories	
32	Should be able to scan SQL Injections for MSSQL and Postgre SQL, databases	
33	Should be able to scan Local file inclusion (LFI), Remote file inclusion (RFI), XSS - Cross Site Scripting & Malware.	
34	The scanning should support\cover following	
	· Open ports scanning for Security Threats	
	· Banner detection, directory scanning & directory indexing.	
	· Full Path disclosure in the pages	
	· Password auto complete enabled fields	
	· Page defacement detection & view state decoder	
	· Password submission method	
	· Time based scanning	
	· Robust link crawler	
	· SSL Certificate checking	
	· Web Shell Locater & Web Shell Finder	
	· Reverse IP domain check	
36	Generate logs for scanner access and testing.	
37	Solution should be a tool based automated solution	
38	Solution should support scanning of static and dynamic links	
39	Solution should be independent of application platform	
40	Malware Monitoring scanning on hourly basis. If any malware is injected into Web Applications, then immediately malware alert message shall be forwarded to authority. Application Audit and Vulnerability assessment of weekly basis.	
41	It should be able to integrate with other security solutions (i.e., Security Information / Event Management, Patch Management, IDS, IPS, etc.)	
42	It should integrate with the existing / proposed WAF solution	
43	24*7 monitoring / scanning of web pages for real time detection of malware injection. No skipping of page scanning.	
44	The service provider should have the ability to provide/Create Users with various privilege levels (view only / View or take down certain incident types)	

9.2.6 Application Performance Monitoring

#	Database Monitoring	Compliance Y/N

1	APM should be able to provide Overview of database server like Database details, version etc.	
2	APM should be able to provide host details which are connected to database Server	
3	APM should be able to provide session details of all active database sessions.	
4	Monitoring & management of network link proposed as part of this solution.	
5	APM should be able to provide server configuration details (All configurations, Advanced Configurations, RECONFIGURE Configurations, Memory Configurations)	
6	Bandwidth utilization, latency, packet loss etc.	
7	APM should be able to provide Jobs and Backup Details, including the following:	
	i) Currently executing Jobs.	
	ii) Job Steps Execution Info.	
	iii) Job Schedule Info.	
	iv) Recent Database Backup.	
	v) Back-Up within Past 24 Hours.	
8	APM should monitor and provide details on the following queries performance parameters:	
	i) Top Queries by CPU, Top Queries by I/O	
	ii) Top Waits by Waiting Tasks, Top Slow Running Queries	
	iii) Most Frequently Executed Queries, Most Blocked Queries	
	iv) Top Queries by Lowest Plan Reuse, Cost of Missing Indexes	
9	APM should provide to set following monitoring parameters for continuous monitoring:	
	i) Total Server Memory, SQL Cache Memory	
	ii) Optimizer Memory, Lock Memory	
	iii) Connection Memory, Target Server Memory	
	iv) Granted Workspace Memory, Buffer Cache Hit Ratio	
	v) Page Lookups/Sec, Pages Read/Sec	

	vi) Page Life Expectancy (ms)	
	vii) User Connections, Logins/Sec	
	viii) Logouts/Sec, Cache Hit Ratio	
	ix) Cache Count, Cache Pages	
	x) Lock Requests/Sec, Lock Wait/Sec	
	xi) Lock Timeout/Sec, Full Scans/Sec	
	xii) Range Scans/Sec, Probe Scans/Sec	
	xiii) Work Files Created/Sec, Worktables Created/Sec	
	xiv) Index Searches/Sec, Latch Waits/Sec	
	xv) Average Latch Wait Time, Batch Requests/Sec	
	xvi) SQL Compilations/Sec, SQL Recompilations/Sec	
	xvii) Auto-Param Attempts/sec, Failed Auto-Params /Sec	
	xviii) Safe Auto-Params/Sec, Unsafe Auto-Params/Sec	
	xix) Availability	
#	Web Service Monitoring	Compliance (Y/N)
1	APM should provide website details hosted on web server.	
2	APM should provide application details running on web server.	
3	Monitoring & management of network link proposed as part of this solution.	
4	Bandwidth utilization, latency, packet loss etc.	
5	APM should consist of the following monitoring parameters:	
	i) Site Status, Total Bytes Sent	
	ii) Bytes Sent/Sec, Total Bytes Received	
	iii) Bytes Received/Sec, Total Bytes Transferred	
	iv) Bytes Total/Sec, Total Files Sent	
	v) Files Sent/Sec, Total Files Received	
	vi) Files Received/Sec, Current Connections	
	vii) Maximum Connections, Total Connection Attempts	
	viii) Total Logon Attempts, Service Uptime	

#	Application	Compliance Y/N
1	APM should consist of the following monitoring parameters:	
	i) Memory Monitoring	
	ii) Web Applications and Deployments	
	iii) Connections, Transactions, Queries	
	iv) Web Metrics	
	v) Transactions	
	vi) Availability	
2	Monitoring & management of network link proposed as part of this solution.	
3	Bandwidth utilization, latency, packet loss etc.	

9.2.7 SIEM Service

#	SIEM Description	Compliance (Y/N)
1	The solution should be able to handle events equal to the events handled by current system	
2	The solution should be scalable by adding additional receivers and still be managed through a single, unified security control panel.	
3	The solution should be capable of real time analysis and reporting.	
4	The platform should not require a separate RDBMS for log collection, web server or any kind of application software for its installation.	
5	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.	
6	The relative risk of each activity should be calculated based on values assigned by the Asset Administrator.	
7	The activities should be separated by levels of risk for the company: very high, high, medium, low and very low.	
8	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.	
9	The solution should be able to collect logs via the following ways as inbuilt into the solution: Syslog, OPSec, agent-less WMI, RDEP, SDEE, FTP, SCP, External Agents such as Adiscon.	
10	The solution should provide a data aggregation technique to summarize and reduce the number of events stored in the master database.	
11	The solution should provide a data store which is compressed via flexible aggregation logic.	
12	The data collected from the receiver should be forwarded in an encrypted manner to SIEM log storage.	
13	The solution should provide pre-defined report templates. The reports should also provide reports out of the box such as ISO 27002.	
14	The solution should provide reports that should be customizable to meet the regulatory, legal, audit, standards and management requirements.	
15	The solution should also provide Audit and Operations based report, Native support for Incident management workflow.	
16	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.	

#	SIEM Description	Compliance (Y/N)
17	A well-defined architecture along with pre and post installation document need to be shared by the bidder.	
18	The solution should have a scalable architecture, catering multi-tier support and distributed deployment.	
19	The solution should support collection of events/logs and network flows from distributed environment(s).	
20	The solution should correlate security/network events to enable the SOC to quickly prioritize it's response to help ensure effective incident handling.	
21	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.	
22	The solution should provide remediation guidance for identified security incident:	
23	Solution should be able to specify the response procedure (by choosing from the SOPs) to be used in incident analysis/remediation.	
24	The solution should facilitate best practices configuration to be effectively managed in a multi-vendor and heterogeneous information systems environment.	
25	The solution should provide capability to discover similar patterns of access, communication etc. occurring from time to time, for example, slow and low attack.	
26	The solution should perform regular (at least twice a year) health check and fine tuning of SIEM solution and should submit a report.	
27	The solution should share the list of out of the box supported devices/log types.	
28	The solution should support hierarchical structures for distributed environments. The solution should have capability for correlation of events generated from multiple SIEM(s) at different location in single management console.	
29	The event correlation on SIEM should be in real time and any delay in the receiving of the events by SIEM is not acceptable.	
30	The solution should support internal communication across SIEM-components via well-defined secured channel. UDP (User Datagram protocol) or similar ports should not be used.	
31	Event dropping/caching by SIEM solution is not acceptable and same should be reported and corrected immediately.	
32	The solution should be able to facilitate customized dashboard creation, supporting dynamic display of events graphically.	
33	The solution should be able to capture all the fields of the information in the raw logs.	
34	The solution should support storage of raw logs for forensic analysis.	

#	SIEM Description	Compliance (Y/N)
35	The solution should be able to integrate logs from new devices into existing collectors without affecting the existing SIEM processes.	
36	The solution should have capability of displaying of filtered events based on event priority, event start time, end time, attacker address, target address etc.	
37	The solution should support configurable data retention policy based on organization requirement.	
38	The solution should provide tiered storage strategy comprising of online data, online archival, offline archival and restoration of data. Please elaborate on log management methodology proposed.	
39	The solution should compress the logs by at least 70% or more at the time of archiving.	
40	The solution should have capability for log purging and retrieval of logs from offline storage.	
41	Solution should be capable of replicating logs in Synchronous as well as Asynchronous mode for replication from Primary site to DR site.	
42	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.	
43	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.	
44	The solution should support automated scheduled archiving functionality into file system.	
45	The solution should support normalization of real time events.	
46	The solution should provide a facility for logging events with category information to enable device independent analysis.	
47	The platform should be supplied on Hardened OS embedded in Hardware / Virtual Appliance. The storage configuration should offer a RAID configuration to allow for protection from disk failure.	
48	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.	
49	By default, at the time of storage, solution should not filter any events. However, solution should have the capability of filtering events during the course of correlation and report generation.	
50	The solution should ensure the integrity of logs. Compliance to regulations should be there with tamper-proof log archival.	
51	The solution should be able to continue to collect logs during backup, de-fragmentation and other management scenarios.	

#	SIEM Description	Compliance (Y/N)
52	The solution should support collection of logs from all the devices quoted in RFP.	
53	The collection devices should support collection of logs via the following but not limited methods:	
	1. Syslog over UDP / TCP	
	2. SNMP	
	3. ODBC (to pull events from a remote database)	
	4. FTP (to pull a flat file of events from a remote device that can't directly write to the network)	
	5. Windows Event Logging Protocol	
	7. NetBIOS	
54	The solution should allow a wizard / GUI based interface for rules (including correlation rules) creation as per the customized requirements. The rules should support logical operators for specifying various conditions in rules.	
55	The solution should support all standard IT infrastructure including Networking & Security systems, OS, RDBMS, Middleware, Web servers, Enterprise Management System, LDAP, Internet Gateway, Antivirus, and Enterprise Messaging System, Data loss prevention (DLP), etc.	
56	Solution should have license for minimum 10 users for SIEM administration.	
57	The solution should have the ability to define various roles for SIEM administration, including but not limited to: Operator, Analyst, SOC Manager etc. for all SIEM components.	
58	The solution should support SIEM management process using a web-based solution.	
59	The solution should support the following co- relation: 1.2. Statistical Threat Analysis - To detect anomalies. 1.3. Susceptibility Correlation - Raises visibility of threats against susceptible hosts. 1.4. Vulnerability Correlation - Mapping of specific detected threats to specific / known vulnerabilities. 1.5. Rules based Correlation - The solution should allow creating rules that can take multiple scenarios like and create alert based on scenarios.	
60	Solution should have capability to correlate based on the threat intelligence for malicious domains, proxy networks, known bad IP's and hosts.	

#	SIEM Description	Compliance (Y/N)
61	The solution should provide ready to use rules for alerting on threats e.g., failed login attempts, account changes and expirations, port scans, suspicious file names, default usernames and passwords, High bandwidth usage by IP, privilege escalations, configuration changes, traffic to non-standard ports, URL blocked, accounts deleted and disabled, intrusions detected etc.	
62	The solution should support the following types of correlation conditions on log data: a) One event followed by another event b) Grouping, aggregating, sorting, filtering, and merging of events. c) Average, count, minimum, maximum threshold etc.	
63	Solution should provide threat scoring based on: a) Host, network, priority for both source & Destination b) Real-time threat, event frequency, attack level etc.	
64	The solution should correlate and provide statistical anomaly detection with visual drill down data mining capabilities.	
65	The solution should have the capability to send notification messages and alerts through email, SMS, etc.	
66	The solution should support RADIUS and LDAP / Active Directory for Authentication.	
67	The solution should provide highest level of enterprise support directly from OEM.	
68	The solution should provide a single point of contact directly from OEM for all support reported OEM.	
69	The solution should ensure continuous training and best practice updates for onsite team from its backend resources.	
70	Solution should support log integration for IPv4 as well as for IPv6.	
71	Solution should provide inbuilt dashboard for monitoring the health status of all the SIEM components, data insert/retrieval time, resource utilization details etc.	
72	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.	
73	The central management console/ Enterprise Security managers/receivers should be in high availability.	
74	24/7 extensive monitoring of the cloud services and prompt responses to attacks and security incidents	
75	Recording and analyzing data sources (e.g., system status, failed authentication attempts, etc.)	
76	24/7 contactable security incident handling and troubleshooting team with the authority to act	

#	SIEM Description	Compliance (Y/N)
77	Obligations to notify the customer about security incidents or provide information about security incidents potentially affecting the customer	
78	Provision of relevant log data in a suitable form	
79	Logging and monitoring of administrator activities	

9.2.8 Backup solution

S.No.	Description	Compliance (Y/N)
1	The proposed backup solution should have broad platform support - such as Windows, RHEL, SLES, Oracle Linux, Ubuntu, Dabian,Solaris,AIX,HP-UX, Freebsd,Vmware,HyperV,Nutanix,KVM, Oracle DB, MS-SQL, SAP HANA, Exchange, Sharepoint, M365/O365 and NDMP, NFS,SMB backups.	
2	The proposed backup solution should support internal HA mechanism allowing to achieve high availability of backup environment without any dependencies on any other vendor. Bidder to provide complete details to enable high availability of backup environment.	
3	The proposed cloud console must be provided with the cloud console.	
4	The proposed software should provide a remote deployment gateway to establish a secured connection between a all instances which needs to be considered for backup with cloud console.	
5	The proposed backup solution should be provided to take 2 AWS Virtual Machines. In event, if support tenure gets expired then still it should not affect the backup or restore operations. The backup solution should allow to perform disk-to-disk backup and tape out also integrate with S3-compliant cloud buckets for long archival of backup data.	
6	The proposed backup solution should allow incremental backup to reduce backup overhead and each backup image copy should allow granular file/folder to restore and complete VM recovery.	
7	The proposed backup solution should not be dependent on external backup proxy to initiate VM backup and should support complete VM recovery, Granular VM recover, Instant VM and automate VM restore in hypervisor VM repository for critical VMs. For physical servers, its should support complete bare metal recovery on similar and dis-similar hardware.	
8	The proposed backup solution should provide mechanism to validate backup image before restoring the backup to ensure only clean backup images gets restore.	
9	The proposed solution should have support for Multiplexing and Multi streaming to accelerate and scale performance in any environment.	
10	The proposed solution should have single console for disc based, tape based and cloud-based backups.	

11	Proposed solution should have Catalogs and a central Database for quickly find backups and files without recalling tapes or pulling data from the cloud. The catalogs must be stored on SSD disks and backup data must be stored on NL-SAS disks. The SSD and NL-SAS disk must have disk failure consideration to avoid any data loss due to disk failures.	
12	Proposed solution should have multi-tier modular architecture.	
13	Proposed solution should have infrastructure visualization to simplify system management with an easy-to-read network diagram view of your environment.	
14	The proposed solution must provide deduplication across backup job, daily, weekly, monthly backup	
15	The proposed solution must include inbuild source and destination deduplication technology. Backup solution should not depend on external storage to perform deduplication.	
16	The proposed solution must have the ability configuring same destination target volume with deduplication or non-deduplication.	
17	The proposed solution must have the ability to show in report individual server deduplication rate, storage used for each individual backup.	
18	The proposed solution must support hardware snapshot backup to various popular storages e.g NetApp, HPE 3PAR, Nimble and integrate with Nutanix Files.	
19	The proposed backup solution should provide testing mechanism to backup images without any human interventions and provide report.	
20	The proposed solution must provide the ability to perform Adhoc Assured Recovery, i.e. rerun Adhoc Assured Recovery of all the backup image.	
21	The proposed solution must support AES 256 encryption for data on move and at rest	
22	The backup solution should have robust Bare metal recovery from physical servers to Virtual, virtual to virtual, virtual to physical and physical to physical.	
23	The backup solution must have option to perform complete VM recovery using Virtual Standby option providing instance recovery in DC and DR site. Virtual Standby to be used for DR replication in another region of AWS/Azure/GCP. Virtual Standby should allow to perform failover and failback without restricting for private or public cloud.	
24	The backup solution should be architected with cloud-native capabilities and should be integrated with both on-site and off-site disaster recovery with built-in cloud DR and backup to private and public clouds including Amazon AWS, Microsoft Azure and other 3rd party compatible clouds.	
25	The proposed backup solution shall provide block level Global & Source side de-duplication to drastically reduce storage & network needs with bandwidth throttling support to reduce WAN utilization.	
26	The proposed backup solution must support configurable block size for de-duplication. The block size must be able to configure as small as 4K block for best deduplication ratio to max of 64K blocks.	

27	The proposed backup solution should have Role-based administration and it should integrate with Active Directory. The backup solution should provide role-based access control to help delegate specific privileges to users.	
28	The proposed backup solution should provide additional security using 2FA / MFA for the backup application console to restrict un-authorized access to the backup management console.	
29	The proposed backup solution should provide security dashboard and allow/block known and unknown applications with cybersecurity solution that includes: (a) Signature-based and signatureless next-gen machine-learning AV engine (b) behavior analysis for ransomware detection and protection with encryption rollback (c) Category-based application control and whitelisting (d) Peripheral device control and much more	
30	The proposed backup solution should be provided with min. three years 24x7 support.	
31	The proposed backup solution should provide unlimited support ticket, bug-fixes support.	
32	The proposed backup solution should provide support from center available in India so no dependencies of language or accent while getting the support.	

9.3. Pre-Qualification Cover Letter

(To be submitted on the letterhead of the bidder)

[Date]

To

System Manager

CIDCO, Telecom Department,

CIDCO Bhavan, CBD Belapur,

Navi Mumbai - 400 614

Subject: Submission of proposal in response to the RFP for "Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO"

Ref:

Dear Sir,

Having examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the professional services as required and outlined in the RFP for the Appointment of Service Provider for the Project "Request for Proposal for Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO."

We attach hereto our responses to pre-qualification requirements and technical & commercial proposals as required by the RFP. We confirm that the information contained in these responses or any part thereof, including the exhibits, and other documents and instruments delivered or to be delivered to CIDCO, is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the CIDCO in its short-listing process.

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

We agree for unconditional acceptance of all the terms and conditions set out in the RFP document and also agree to abide by this tender response for a period of 180 days from the date of submission of bid. We hereby declare that in case the contract is awarded to us, we shall submit the contract performance guarantee bond in the form prescribed the RFP.

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

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

Signature of Authorized Signatory (with official seal)

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

9.4. Power of Attorney

(To be submitted on an INR 100/- Stamp paper along with the Board Resolution)

Know by all men by these presents, We……..(Name of the Bidder and address of their registered office) do hereby constitute, appoint and authorize Mr. / Ms. ……(name and residential address of Power of attorney holder) who is presently employed with us and holding the position of ……..
as our Attorney, to do in our name and on our behalf, all such acts, deeds and things necessary in connection with or incidental to our Proposal for the "Request for Proposal Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO" including signing and submission of all documents and providing information / responses to CIDCO, representing us in all matters before CIDCO, and generally dealing with CIDCO in all matters in connection with our Proposal for the said Project.

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

For _____

Name:

Designation:

Date:

Time:

Seal:

Business Address:

Accepted,

…….. (Signature)

(Name, Title and Address of the Attorney)

Note:

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

The Power of Attorney shall be provided on ₹100/- stamp paper.

The Power of Attorney should be supported by a duly authorized resolution of the Board of Directors of the Bidder authorizing the person who is issuing this power of attorney on behalf of the Bidder.

9.5. Format for Furnishing General Information

The Table below provides the format in which general information about the Bidders must be furnished.

GENERAL INFORMATION			
PARTICULARS	**DETAILS TO BE FURNISHED**		
Details of the Bidder (Company)			
Name			
Address			
Telephone		Fax	
E-mail		Website	
Status of Firm/ Company	(Public Ltd., Pvt. Ltd., etc.)		
Year of Establishment			
Date of registration			
ROC (Registrar of Companies) Reference No.			
Details of company registration			
Company's GST Registration No.			
Company's Permanent Account Number (PAN)			
Name change/ Merger/De-Merger of the organization in last 7 years (Y/N)			
Company's Turnover for last 3 years (Year wise)			
FY 2019– 20	**FY 2020 - 21**	**FY 2021-22**	
Details of Authorized Signatory			
Name			
Address			

Telephone		Fax	
Email			
Details of Contact Person			
Name			
Address			
Telephone		Fax	
Email			

Please submit the relevant proofs for all the details mentioned above along with your Bid response.

Authorized Signatory Signature

Name

Seal

9.6. Declaration of not being banned/debarred/blacklisted by any Government Organization

(Company letterhead)

[Date]

To

System Manager

CIDCO, Telecom Department,

CIDCO Bhavan, CBD Belapur,

Navi Mumbai - 400 614

Sir,

Sub: Declaration of not being banned or debarred by any Government Organization

I _____, authorized representative of _____, hereby solemnly confirm that the Company ……..is not banned/debarred/blacklisted by any Government Organization which includes any Government Department, Public Sector Undertakings of the Government, Statutory Boards formed by the Government, Local Bodies in the State, Co-operative Institutions in the State, Universities and Societies formed by the Government for any reason as on last date of submission of the Bid. In the event of any deviation from the factual information/ declaration, CIDCO reserves the right to reject the Bid or terminate the Contract without any compensation to the Company.

Thanking you,

Yours faithfully

(Signature of the Authorized signatory of the Bidding organization)

Name :
Designation :
Date :
Time :
Seal :
Business Address :

9.7. Annual Turnover Format

Annual Turnover for last 3 financial years (FY 20-21, FY 21-22, FY 22-23) from the field of website design and development and cloud service.

NAME OF BIDDER: <<Company Name>>

Details	FY' 2020– 21	FY' 2021 - 22	FY' 2022-23
Turnover from the field of website design and development and cloud service			
Average Annual Turnover			

- The information supplied shall be substantiated by data in the audited balance sheets and profit and loss accounts for the relevant years and submitted as attachments in respect of the selected Bidder.
- Contents of this form should be certified by Chartered Accountant of the Bidder.

9.8. Details of Experience

Summary of Projects quoted for consideration for Pre-Qualification Evaluation must be filled in the following Format:

Ref No. PQ#	Name of Project and Client Name	Client Type (Private / Govt/ PSUs/ Semi Govt/ ULBs/ Statutory bodies)	WO/PO/Agreement date	Project Value (in INR Crores)	Status (On-Going/ Completed)	Work Order Page No	Client/ Self Certificate – Page No

Additionally, details of each of the Projects mentioned above for consideration must be provided in Format below:

S. No	Information Sought	Information
•	Client's name	
•	Assignment/Job name	
•	Contact Details of the Client	
•	Description of Project	
•	Role of Services as provided by your firm under the contract	
•	Scope of Services as provided by your firm under the contract	
•	Technologies Used	
•	Outcomes of the Project	
•	Current Status (Completed / Phase Completion)	
•	Duration of Assignment/Job (Months)	
•	Value of the contract (In Indian National Rupees)	
•	Start date (Month/Year)	
•	Completion date (Month/Year) / On-Going	
•	Copy of Work Order or PO or Client Certificate or Certificate from Company Secretary	
•	Copy of Completion/ Milestone / Self Certificate	
•	Any other Supporting Document	
•	Mention criteria under which this project is being cited (Refer point No. 1 of the note below)	
Signature of Bidder:		
Date:		
Place:		

Note:

- The Bidder shall attach copies of Certificate of Completion/Substantial Completion issued by the Employer or the self-declaration with the form, failing which the claim of the Bidder shall be liable to be rejected.
- All the fields are mandatory to be filled.

(Signature of the Authorized signatory of the Bidder)
Name:
Designation:
Seal:

9.9. Authorization from OEM/successful bidder

(OEM/successful bidder letterhead)

[Date]

To

System Manager

CIDCO, Telecom Department,

CIDCO Bhavan, CBD Belapur,

Navi Mumbai - 400 614

Sub: Authorization of <Company name of Bidder> to provide services based on our product(s)

Sir,

This is to certify that I/We are the Cloud service provider in respect of the services listed below. I/We confirm that <name of Bidder> ("Bidder") have due authorization from us to provide services, to CIDCO, that are based on our product(s)/services listed below as per "Request for Proposal Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO" in CIDCO. We further endorse the warranty, contracting and licensing terms provided by Bidder to CIDCO.

Sr. No	Product Name	Remarks

Yours faithfully,

Authorized Signatory

Designation

Date

Time

Seal

Business Address

OEM's company name

CC: Bidder's corporate name

9.10. Professional resources details

The following are minimum qualifications and experience for key resources required to implement the cloud solution. The following personnel would be required during the Design, Migration, Configuration, Installation and Setup of the Cloud solution . The Project Manager would continue during the post implementation project management phase.

#	Role	Minimum Qualification & Experience
1	Project Lead	• B. Tech / B. E in CS/IT/EE or MCA; with 7 years of IT experience Or Any Graduate with 9 years of e-Governance Experience
2	System/cloud Administrator	• B. Tech / B. E in CS/IT/EE or MCA; With 4 years of IT experience and having certifications like MCSE/RHCE/RHEL Or Any Graduate having 7 years of IT experience with certifications like MCSE/RHCE/RHEL
3	Senior Software Developer	• B. Tech / B. E in CS/IT/EE or MCA; With 4 years of IT experience Or Any Graduate having 7 years of IT experience
4	Software Developer or UI/UX Developer	• B. Tech / B. E in CS/IT/EE or MCA; With 2 years of IT experience Or Any Graduate having 5 years of IT experience
5	Database Administrator	• B. Tech / B. E in CS/IT/EE or MCA; with 4 years of ITexperience & certifications like OCA- DBA/OCP-DBA/MCDBA Or Any Graduate having 7 years of ITexperience with certifications like OCA-DBA/OCPDBA/MCDBA

9.11. Undertaking on Key Personnel

(Company letterhead)

[Date]

To

System Manager

CIDCO, Telecom Department,

CIDCO Bhavan, CBD Belapur,

Navi Mumbai - 400 614

Sub: Undertaking on Key Personnel proposed for the Project

Sir,

1. I/We as Agency do hereby undertake that those persons whose profiles were part of the basis for evaluation of the bids, hereby referred to as "Key Personnel" of the proposed team, shall be deployed during the Project as per our Bid submitted in response to the RFP.

2. We undertake that any of the identified "Key Personnel" shall not be removed or replaced without the prior written consent of CIDCO except where such removal and/or replacement becomes necessary due to exceptional circumstances like disability, resignation, termination, death, etc. of the resource

3. Under exceptional circumstances, if the key personnel are to be replaced or removed, we shall put forward the profiles of personnel being proposed as replacements, which will be either equivalent or better than the ones being replaced. However, whether these profiles are better or equivalent to the ones being replaced will be decided by CIDCO.

4. CIDCO will have the right to accept or reject these substitute profiles.

5. We also undertake to staff the Project with competent team members in case any of the proposed team members leave the Project either due to voluntary severance, disciplinary actions against them or any other reason.

6. We acknowledge that CIDCO has the right to seek the replacement of any member of the Project team being deployed by us, based on the assessment of CIDCO that the person in question is

incompetent to carry out the tasks expected of him/her or found that person does not really possess the skills /experience/qualifications as Projected in his/her profile or on the ground of security concerns or breach of ethics.

7. In case we assign or reassign any of the team members, we shall be responsible, at our expense, for transferring all appropriate knowledge from personnel being replaced to their replacements within a reasonable time. We shall also ensure that such replacements do not adversely impact the quality and timeliness of the Project at any time.

Yours faithfully,

Authorized Signatory

Name :

Designation :

Date :

Time :

Seal :

Business Address:

9.12. CV Format for Resources

1.	Proposed Position		
2.	Name of Firm		
3.	Name of Staff		
4.	Date of Birth		
5.	Nationality		
6.	Total Experience		
7.	Relevant Experience		
8.	Relevant Certification		
9.	Education		
Name of Institution		Degree(s) or Diploma(s) obtained:	Date
10.	Membership in Professional Associations/ Trainings attended		
11.	Countries of Work Experience:		
India			

12.	Languages	
13.	Employment Record:	
From:		To:
Employer		
Position/S Held		
From:		To:
Employer		
Position/S Held		
14.	Work Undertaken that Best Illustrates Capacity to Handle the Tasks Assigned	
	Name of assignment or project:	
	Year:	
	Location:	
	Client:	

	Position/s held:	
	Main project features:	
	Activities performed:	
	Name of assignment or project:	
	Year:	
	Location:	
	Client:	
	Position/s held:	
	Main project features:	
	Activities performed:	

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

Date:

Full name & Signature of authorized representative:

9.13. Format for Performance Bank Guarantee

PROFORMA OF PERFORMANCE BANK GUARANTEE

(On Stamp Paper of Rs.100/- as per Maharashtra Stamp Act, 1958 and as amended from time to time from Nationalized/Scheduled Banks operable in Mumbai or Navi Mumbai only)

To,
City & Industrial Development Corporation of Maharashtra Limited.
`Nirmal', 2nd floor. Nariman Point,
Mumbai 400 021.

In consideration of the City and Industrial Development Corporation of Maharashtra Limited, a Company incorporated under the Companies Act, 1956 (1 of 56) and having its registered office at Nirmal, 2" floor, Nariman Point, Mumbai - 400 021 (hereinafter called the 'Employer' which expression shall unless repugnant to the subject or context and meaning thereof include its successors and assign) having agreed under the terms and conditions of Contract Agreement No._____ dated _____ made between M/s. _____ (Name of Agency) (hereinafter called the 'Contractor' which expression shall unless repugnant to the subject or context and meaning thereof include his heirs, executors administrators and assigns / its successors and assign) and the Employer in consideration with _____ (Name of Work) (hereinafter called "the said Contract") to accept a deed of Guarantee as herein provided for ₹ _____ by _____(Name of the Nationalized/ Scheduled Bank, Mumbai /Navi Mumbai Branch) towards unbalance bid, for the due fulfilment by the Contractor of the terms and conditions contained in the said contract. We, _____ (Name of Bank and detailed address) the Bank constituted and established under the Banking Companies (Acquisition and transfer of undertakings) Act, 1979 (hereinafter referred to as the 'said Bank') and having our Head Office at _____ (Address) at the request of M/s _____ (Name of Agency) do hereby undertake to pay to the Employer an amount not exceeding ₹ _____ (Rupees _____) only against any loss or damage caused to or suffered or would be caused to or suffered by the Employer by reasons of any breach by the said Contactor(s) of any of the terms or conditions contained in the said Contract Agreement and to unconditionally pay the amount claimed by the Employer on demand and without demur to the extent expressed.

We, _____ (Name of Bank) do hereby undertake to pay amounts due and payable under this guarantee without any demur, merely on a demand from the Employer stating that the amount claimed is due by way of loss or damage caused to, or would be caused to or suffered by the Employer by reason of breach by the said Contactor(s) of any of the terms or condition contained in the said Contract Agreement or by reasons of the Contractor(s) failure to perform 'the said Contract Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding ₹_____ (Rupees _____ only)

We, _____ (Name of Bank) Further agree that the Employer shall be the sole judge of and as to whether the Contactor has committed a breach of any of the terms and conditions of the said Contract and the extent of the loss, damage, costs, charges and expenses caused to or suffered by or that may he caused to or suffered by the Employer on account thereof and the decision of the Employer that the Contractor has committed such breach and as to the amount or amounts of loss, damage, costs, charges and expenses caused to or suffered by or that may be caused to or suffered by the Employer from time to time shall be final and binding on us.

We undertake to pay the Employer any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s)/ Supplier(s) in any suit or proceeding pending before any court of Tribunal unequivocal, without demur. The payment so made by us under this bond shall be a valid discharge of our liability for payment thereunder and the Contractor(s) / Supplier(s) shall have no claim against us for making such payment.

We, _____ (Name of Bank) further agree that the guarantee herein contained shall remain in full force and effect during the Contract Period including Extensions in time limit if any & also till such time the Taking Over Certificate is issued for the whole completed work including that would be taken from the performance of the said Agreement and shall continue to be enforceable till all the dues of the Employer under or by the said Agreement have been fully paid and its claims satisfied or discharged or till the _____(indicate the Systems Manager, CIDCO Limited) certified that the terms and conditions of the said Contract Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this guarantee. Unless a demand or claim under this guarantee is made on us in writing on or before _____ (contract period + claim period) we shall be discharged from all liability under this guarantee thereafter.

We, _____, further agree with the Employer, that the Employer shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Agreement or to extend the time of performance by the said Contractor(s) from time to time or to postpone for any time any of the powers exercisable by the Employer against the said Contractor(s) and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reasons of any such variation, or extension being granted the said Contractor(s) or for any forbearance act or omission on the part of the Employer or any indulgence by the Employer to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provisions have effect of so relieving us

This guarantee will not be discharged due to the change in the constitution of the Bank or the Contractor(s) Supplier(s).

This guarantee is valid till _____ (completion date) unless a suitable action to enforce the claim under this guarantee is made within six months from completion date i.e., up to _____ (date) all yours rights under this guarantee shall he forfeited, and we shall be relieved and discharged from all liabilities there under.

We, _____ (Name of Bank) lastly undertake not to revoke this guarantee during the currency except with the previous consent of the Employer in writing.

Date this _____ day of _____ 2023

Dated this _____ day of _____ 2023.

FOR & ON THE BEHALF OF BANK

The above guarantee is accepted.

For and on behalf of the Employer

(Name & Designation)

Date:

9.14. Technical Bid Cover Letter

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

[Date]

To

System Manager

CIDCO, Telecom Department,

CIDCO Bhavan, CBD Belapur,

Navi Mumbai - 400 614

Sub: Submission of proposal in response to the RFP for Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO

Ref: XXXXXXXXX

Dear Sir,

Having examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the professional services as required and outlined in the RFP for Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO.

We attach hereto the technical response as required by the RFP, which constitutes our proposal. We undertake, if our proposal is accepted, to adhere to the proposed plan (Project schedule) for providing Professional Services in Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO, put forward in RFP or such adjusted plan as may subsequently be mutually agreed between us and CIDCO or its appointed representatives.

If our proposal is accepted, we will obtain a Performance Bank Guarantee issued by a nationalized bank in India, for a sum of equivalent to 3% of the contract value for the due performance of the contract.

We agree for unconditional acceptance of all the terms and conditions set out in the RFP document and also agree to abide by this tender response for a period of 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 contract is prepared and executed, this tender response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and CIDCO.

We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules, and other documents and instruments delivered or to be delivered to CIDCO 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 CIDCO as to any material fact.

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

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

Date: (Signature) (Name)	Witness Signature:
(In the capacity of)	Witness Name:
[Seal / Stamp of bidder]	Witness Address:

CERTIFICATE AS TO AUTHORISED Successful Bidder

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

Date:

Signature:

(Company Seal) (Name)

9.15. Format for Commercial Proposal

Format 1- Commercial bid letter

To

System Manager

CIDCO, Telecom Department,

CIDCO Bhavan, CBD Belapur,

Navi Mumbai - 400 614

Email: sm.dc@cidco.maharashtra.gov.in

Subject: Request for Proposal for "Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO.

Ref: Tender No: XXXXXXXXX Dated: XX/XX/XXXX

Dear Sir,

We, the undersigned Bidder, having read and examined in detail all the Tender documents in respect of Appointment of an Agency for CIDCO website migration, revamp/redesign and hosting in cloud environment along with providing cloud infrastructure and annual maintenance for three years do hereby propose to provide services as specified in the Tender documents number XXXXXXXXX Dated XX/XX/XXXX

PRICE AND VALIDITY

- All the prices mentioned in our Tender are in accordance with the terms as specified in the Tender documents. All the prices and other terms and conditions of this Tender are valid for a period of 120 calendar days from the date of opening of the Tenders.
- We hereby confirm that our Tender prices include all taxes. Taxes are quoted separately under relevant sections, as specified in the RFP formats.
- 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.

UNIT RATES

We have indicated in the relevant schedules enclosed, the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

DEVIATIONS

We declare that all the services shall be performed strictly in accordance with the RFP 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.

Further we agree that additional conditions, if any, found in our bid documents, other than those stated in the deviation schedule in Pre-Qualification Envelope, shall not be given effect to.

QUALIFYING DATA

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

BID PRICE

We declare that our Bid Price is for the entire scope of the work as specified in the RFP documents. These prices are indicated in the subsequent sub-sections of this Section.

CONTRACT PERFORMANCE GUARANTEE BOND

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

We hereby declare that our Tender 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 Tender is binding on us and that you are not bound to accept a Tender you receive. We confirm that no technical deviations are attached here with this commercial offer.

Thanking you,

Yours faithfully,

(Signature of the Bidder) Name

Designation Seal

Date:

Place:

Business Address:

Summary of Commercial Proposal

Table: 1

Sr. No	Item	Ref. Schedule	Total Price
1	Website Migration Cost		
2	Website revamp/redesign and deployment cost	A	
3	Website maintenance for three years	B	
4	Cloud infrastructure and services cost for three years	C	
Total			
Grand Total in Words			

Bidders shall be evaluated by the quotes submitted as per table 1.

Schedule A- Website revamp/redesign and deployment cost

Sr. No.	Parameter	Year 1	Year 2	Year 3	Total
1.	Redesign, development & implementation of website with all modules as mentioned in this RFP.		NA	NA	
2.	Total				

Schedule B- Website maintenance for three years from project initiation

Sr. No.	Resource	Qualification	Number of resources	Year1	Year2	Year3	Total
1	Senior Software Developer	B. Tech / B. E in CS/IT/EE or MCA; With 4 years of IT experience Or Any Graduate having 7 years of IT experience out of which 5 years should be in Government domain.	3				
Total Amount for 3 years							

Note: Any additional service required for smooth maintenance of website should be given by the back office at no cost to CIDCO.

Schedule C- Cost for cloud infrastructure.

Sr. No.	Parameter	Server Config	Qty.	Unit Price in INR (Exclusive of Taxes) (A)	Taxes and charges	Year1	Year2	Year3	Total
1	CPU and RAM	8 vCPUs, 64 GB RAM	4						
	Storage	256 GB SSD							
	Operating System	Any OS as per requirement							
	Incremental Back Up	Yes							
2	CPU and RAM	16vCPUs, 64 GB RAM	2						
	Storage	256 GB SSD							

Sr. No.	Parameter	Server Config	Qty.	Unit Price in INR (Exclusive of Taxes) (A)	Taxes and charges	Year1	Year2	Year3	Total
	Operating System	Any OS as per requirement							
	Incremental Back Up	Yes							
3	DR as a Service	Per Device	3						
4	Extra Storage Disk across all VM (BLOB up to 2000 IoPS)	in TB	1						
5	Backup (Archival Storage)	in TB	1						
6	Backup Agent	per VM (device)	3						
7	Public IP	For each app VM	4						
8	Bandwidth	100 GB/Month	1						
9	Web Application Firewall (WAF)	Per FQDN per month	1						
10	Firewall as a Service for DC and DR in HA (incl. 5VPN clients with MFA)	Instance	4						
11	SSL (Wildcard)	1 for all servers	1						

Sr. No.	Parameter	Server Config	Qty.	Unit Price in INR (Exclusive of Taxes) (A)	Taxes and charges	Year1	Year2	Year3	Total
12	Load Balancer as a service	-	1						
13	DDOS as a Service	Mbps	20/50						
14	Endpoint Security for Servers	Per Device							
15	<Include DR VMs>	Hourly							
16	Any other line item								
17	**Total Amount for 3 years**								

9.16. Common guidelines / comments regarding the compliance of IT / Non-IT Equipment / Any new Systems to be procured.

1) The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. Bidders are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.
2) All IT Components should support IPv4 and IPv6
3) The Successful bidder should also propose the specifications of any additional servers / other hardware, if required for the system.
4) Any new Servers provided should meet industry standard performance parameters (such as CPU Utilization of 60% or less, disk utilization of 75% or less). In case any non-standard computing environment is proposed (such as cloud), detail clarification needs to be provided to confirm a) how the sizing has been arrived at and b) How SLAs would be met.
5) Successful Bidder is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) to affect the performance / SLAs.
6) Any additional hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). CIDCO reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all requirements specified in tender documents.
7) All licenses should be in the name of CIDCO, Navi Mumbai.

CITY AND INDUSTRIAL DEVELOPMENT CORPORATION OF MAHARASHTRA LIMITED

(Government of Maharashtra Undertaking)

Request for Proposal for Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO

CIDCO Bhavan, CBD-Belapur, Navi Mumbai-400614

Ref No.: 05/CIDCO/SD/SM/2023-24/ Corrigendum-1

CIDCO Limited
Systems Manager,
Systems Department
First Floor, CIDCO Bhavan
CBD Belapur, Navi Mumbai - 400 614
Contact number: 022-67918699
Fax: 022-67918166

1. Clarifications for queries received on RFP.

The following clauses of the RFP is amended/modified, and to be read as under:

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
1	7.1.1. Mandatory Eligibility Criteria (Pre-qualification Criteria)	67	**As per clause PQ6: Similar Experience** The bidder must have experience in projects related to IT related services involving Design Development, Implementation and Maintenance of an official Website implementation or maintenance of cloud infrastructure service in Govt./Semi. Govt. sectors / PSUs in last 5 years as on bid submission date: At least one (01) project (which includes development & maintenance of web application) of value not less than INR 3.4crore OR At least two (02) projects (which includes development & maintenance of web application), each of value not less than INR 2.5crore OR At least three (03) projects (which includes development & maintenance of web application), each of value not less than INR 1.7crore	**Request to add as below:** The bidder must have experience in projects related to IT related services **and Data Centre with allied works** involving Design Development, Implementation and Maintenance of an official Website implementation or maintenance of cloud infrastructure service in Govt./Semi. Govt. sectors / PSUs in last 5 years as on bid submission date: At least one (01) project (which includes development & maintenance of web application) of value not less than INR 3.4crore OR At least two (02) projects (which includes development & maintenance of web application), each of value not less than INR 2.5crore OR At least three (03) projects (which includes development & maintenance of web application), each of value not less than INR 1.7crore	As per RFP. Bidders who experience in providing only cloud services will not be considered.

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
2	7.1.1. Mandatory Eligibility Criteria (Pre-qualification Criteria)	68	**As per clause PQ 10: Certification** The bidder should have an ISO 9001:2015, ISO: 27001 certification and should be an SEI CMM Level 3 or above certified organization.	**Request to modify as below: (Remove "SEI"):** The bidder should have an ISO 9001:2015, ISO: 27001 certification and should be **a CMM Level 3** or above certified organization.	The bidder should have an ISO 9001:2015, ISO: 27001 certification and should be a CMM Level 3 or above certified organization.
3	6 Instruction to Bidders	65	Consortium / Joint Venture is NOT allowed for the purpose of this bid	Can you please change the clause & allow us for consortium?	As per the RFP
4	9.2. Successful bidder's Technical and Functional Compliance	111	Backup Solution	MAF Should be compulsory	As per the RFP
5	9.2. Successful bidder's Technical and Functional Compliance	111	Backup Solution	Separate Price line item in BOQ	As per the RFP
6	9.2. Successful bidder's Technical and Functional Compliance	111	Backup Solution	It Should be Named As ARCSERVE Backup Solution	As per the RFP
7	7. Bid Opening and Proposal Evaluation Process	66	PQ-4Average annual Turnover of the cloud service provider should be at least INR 1000 Crores for last three financial years.	CSP with 1000 cr turnover would be very difficult for any Indian company hence we request to dilute the turnover criteria to 50 cr for CSP.	As per the RFP

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
8	5.Scope of Work	18	Online payment service platform - 1. Service Charges 2. Water Charges 3. Marketing plot payment 4. Marketing I & II payment 5. Marketing housing and shop payment 6. Station complex service charge payment 7. NIAMS payment 8. Estate. Misc. receipt payment 9. Copas BP/TP 10. Challan payment-misc. water charges 11. Swapnapurti Payment	Can you please elaborate on how the Payments feature work. As per the current website we notice that the website has an option to search using challan or reference numbers. What is the source of the Challan / Reference numbers which the users have to input & verify before making the payment? Are the Challan / Reference numbers created, imported manually or fetched through external system via API integration?	CIDCO will share the requested details with the selected bidder only post onboarding
9	5.Scope of Work	18	Online payment service platform	How is the late fee added to the total challan value once the payment date is passed? How is the late fee configured?	CIDCO will share the requested details with the selected bidder only post onboarding
10	5.Scope of Work	15	MIS Reporting	MIS - Please specify a number and types of reports	The Website shall provide an interface to the CIDCO to obtain the transaction history, summary, and detailed reports on daily transactions, pending applications etc. Additional details will be shared by CIDCO with the selected bidder only post onboarding

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
11	5.Scope of Work	15	Integration of e-forms with online service applications	Since the section has been described as "Integration of eforms" it is assumed that the "eforms" are a third party integration and only the integration is to be considered in scope. The actual development efforts of eforms is not part of the scope. Please clarify.	The design, development, and integration of the e-forms of online services, wherever necessary, are part of the scope.
12	5.Scope of Work	16	Specific Requirements for the Website	What are the different CIDCO user roles that are accessing the CMS in the website?	CIDCO will share the requested details with the selected bidder only post onboarding
13	5.Scope of Work	16	Specific Requirements for the Website	Is the Login / registration feature to be provided for the end users? What are the features accessible to the Logged in Users?	Secure login must be provided to the end users as mentioned in the RFP. Additionally, CIDCO will share the requested details with the selected bidder only post onboarding
14	5.Scope of Work	16	User Login Services	For the login services that are as follows, In the current website these link open in an external website / application. It is assumed that the new website will continue to have these links as external applications/ website and any development around the below applications/ website is not part of the scope of this RFP.Please clarify. 1. COPAS 2. NIAMS	CIDCO will share the requested details with the selected bidder only post onboarding

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
				3. Online Grievances Service 4. CIDCO Samwaad 5. Estate Services 6. Mangrove Complaints 7. RTI online	
15	5.Scope of Work	19	Online payment Services platform	Assuming the Payment method needs to support UPI & Wallet modes of payment.	CIDCO will share the requested details with the selected bidder only post onboarding
16	5.Scope of Work	19	Online payment Services platform	Please elaborate about the Payment rules and regulations.	CIDCO will share the requested details with the selected bidder only post onboarding. Subsequently, Payment gateway will be approved by CIDCO.
17	5Scope of Work	18	Online payment Services platform	Assuming for the Payment services, the Application will be integrated with third party payment service providers. Does CIDCO have any preference about such Payment service provider?	CIDCO will share the requested details with the selected bidder only post onboarding
18	5.Scope of Work	40		Please provide the list of notification supported by the push notification service (e.g., SMS, mobile apps, email).	CIDCO will share the requested details with the selected bidder only post onboarding

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
19	5.Scope of Work	76	Payment Terms	Does CIDCO has any timeline for the development and launch of the Website? Any technology preference?	Timelines for development and Go-Live is already mentioned in the RFP. Bidder has to propose the technology stack.
20	5.Scope of Work	23	Migration from SDC to cloud	It is assumed that once the new website is developed, the old data needs to be migrated to the new website. Please specify the size of data to be migrated. Please specify the different type of data to be migrated.	CIDCO will share the requested details with the selected bidder only post onboarding
21	5.Scope of Work	23	Migration from SDC to cloud	Will CIDCO provide the data in a cleansed & structed format for the migration?	CIDCO will share the requested details with the selected bidder only post onboarding
22	5.Scope of Work	23	Migration from SDC to cloud	Please provide the list and details of the Applications that will be hosted on the new Cloud.	CIDCO will share the requested details with the selected bidder only post onboarding
23	5.Scope of Work	23	Migration from SDC to cloud	Please provide the details of infrastructure currently in use for hosting the applications in SDC (vCORES, Memory, Storage, OS version, DB version etc)	CIDCO will share the requested details with the selected bidder only post onboarding
24	5.Scope of Work	23	Migration from SDC to cloud	What will be the total number of users accessing the application and concurrent users	On an average, daily 5000 users (approximately) access the website.
25	6 Instruction to Bidders	65	Sub-contracting should be allowed for CSP/Website	Sub-contracting should be allowed for CSP/Website	As per RFP

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
			development.	development.	
26	5.Scope of Work	23	Migration from SDC to cloud	What is the current platform on which the VMs are running in SDC (Hypervisor- VMware/ Hyper V etc)	CIDCO will share the requested details with the selected bidder only post onboarding
27	Section 6 – Instruction to bidders	67	The bidder must have experience in projects related to IT related services involving design, development, implementation and maintenance of an official website implementation or maintenance of cloud infrastructure service in Government. Semi Government Sector / PSUs in the last 5 years as on bid submission date: At least one (01) project (which includes development and maintenance of web application) of value not less than INR 3.4 cr At least two (02) projects (which includes development & maintenance of web application), each of value not less than INR 2.5 cr At least three (03) projects (which includes development & maintenance of web application), each of value not less than INR 1.7 cr	1. The experience of working in private sector should also be considered with reputed companies. 2. Also, as per MeitY guidelines with respect to project experience: a) One project of similar nature costing not less than the amount equal to 80 – 100% of the estimated value of assignment to be awarded b) Two projects of similar nature costing not less than the amount equal to 50 – 60% of the estimated value of assignment to be awarded c) Three projects of similar nature costing not less than the amount equal to 40-50% of the estimated value of assignment to be awarded 3. Hence, it is requested to relax as follows: a) One project of similar nature costing not less than the amount equal to Rs 3.2 cr (considering EMD is of Rs 4,00,000) b) Two projects of	The bidder must have experience in projects related to IT related services involving design, development, implementation and maintenance of an official website implementation or maintenance of cloud infrastructure service in Government. Semi Government Sector / PSUs in the last 5 years as on bid submission date: At least one (01) project (which includes development/ maintenance/ hosting of web application) of value not less than INR 3.4 cr or At least two (02) projects (which includes development/ maintenance/ hosting of web application), each of value not less than INR 2.5 cr or At least three (03) projects (which

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
				similar nature costing not less than the amount equal to Rs 2cr c) Three projects of similar nature costing not less than the amount equal to Rs 1.6 cr	includes development/ maintenance/ hosting of web application), each of value not less than INR 1.7 cr Work order mentioning works of development/ maintenance/ hosting of web application will be considered
28	Section 6 – Instruction to bidders	71	The bidder must have experience in projects related to design / development / implementation / maintenance of official website projects / IT / ITeS applications and implementation and maintenance of cloud infrastructure service in Government. Semi Government Sector / PSUs in the last 5 years as on bid submission date	To adopt the similar condition as PQ and also allow experience of private sector to be considered. The bidder must have experience in projects related to IT related services involving design, development, implementation and maintenance of an official website implementation or maintenance of cloud infrastructure service in Government. Semi Government Sector / PSUs / Private sector with reputed organisations in the last 5 years as on bid submission date	As per RFP

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
29	7. Bid Opening and Proposal Evaluation Process	76	1. For migration of website and date from existing service provider – within 3 weeks from the late of acceptance of LoA – 60% of migration charges 2. Mock drill and operational acceptance of website – within 6 weeks from the date of acceptance of LoA – 405 of migration charges Website operational acceptance and Go-Live – within 12 weeks from the date of acceptance of LoA – 40% of website revamp cost. 5. Cloud Services – will start from the date of LoA acceptance – quarterly payment after completion of each quarter after deduction of penalties if any Operational and maintenance – will start from the date of operational acceptance and Go Live – quarterly payment after completion of each quarter after deduction of penalties if any	1. High level migration design and FRS – 3 weeks from date of acceptance of LoA – 30% of migration charges 2. Migration of website and data from existing service provider – 8 weeks from date of acceptance of LoA - 30% of migration charges 3. Mock drill and operational acceptance of website – within 9 weeks from the date of acceptance of LoA – 40% of migration charges 4. Finalization and acceptance of SRS for website: 20% pf website revamp cost 5. Finalization and acceptance of UI/UX and wireframe: 20% of website revamp cost 6. Deployment of revamped upgraded website - 20% of website revamp cost 7. Website operational acceptance and Go-Live – within 12 weeks from the date of acceptance of UI/UX or at a mutually agreed timeline after acceptance of UI/UX – 40% of website revamp cost. 8. Cloud Services – will start from the date of LoA acceptance –	As per RFP

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
				quarterly payment after completion of each quarter after deduction of penalties if any. 9. Operational and maintenance – will start from the date of operational acceptance and Go Live – quarterly payment after completion of each quarter after deduction of penalties if any? 10. Is the vendor expected to pay the cloud service provider and other services provider / license providers and then create a single invoice for Cidco? In that case what happens i If there are sudden loads of traffic that cause significant increase in infrastructure requirements, how will bidder be able to pay for such infra cost? Can the bidder charge additionally for such charges?	
30	5.Scope of Work	18	Requirements – Should provide for and allow financial transaction function	Kindly elaborate on list of payment gateways that are acceptable and can be assessed for integration.	CIDCO will share the requested details with the selected bidder only post onboarding
31	5.Scope of Work	18	Payment made should be credited to the proper head of account as per the rules and directives of CIDCO	Kindly elaborate on APIs which will be exposed of the implemented ERP for delivering the required functionality	CIDCO will share the requested details with the selected bidder only post onboarding

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
32	5.Scope of Work	19	The system should allow transaction through approved financial instruments such as Credit Cards, Debit Cards and Online Banking.	1. Kindly elaborate on the envisaged reconciliation process and how it is intended to be handled? 2. Are there any offline payments which are likely to be accepted and do we need to envisage any provision for the same?	CIDCO will share the requested details with the selected bidder only post onboarding
33	7. Bid Opening and Proposal Evaluation Process	76	The successful bidder shall not be entitled to receive any agreed payments upon termination of the contract. However, the CIDCO may consider making a payment for the part satisfactorily performed on the basis of Quantum Merit as assessed by it if such part is of economic utility to the CIDCO. Applicable under such circumstances, upon termination, the CIDCO may also impose liquidated damages. The successful bidder will be required to pay any such liquidated damages to CIDCO within 30 days of termination date.	Kindly elaborate the quantum and mechanism of calculation of liquidated damages?	CIDCO will share the requested details with the selected bidder only post onboarding

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
34	5 Scope of Work	13	Website architecture	Kindly provide the current website architecture along with integration with different internal applications What is current DB architecture? What is size of current DB/storage across various applications? Please elaborate various file type stored with their purpose. Where is current storage and how can it be accessed for migration? Is there any network connectivity bottleneck that needs to be solutioned for? Please elaborate various software stack used with their versions and purpose of usage. What is current traffic on website in request/sec? What is current write (DB DML changes) traffic on website in request/sec? What is estimated traffic on website in request/sec for next 3/5 yrs? Is there any seasonal high/low period of traffic? Is there any external services used? if yes, which and why?	CIDCO will share the requested details with the selected bidder only post onboarding

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
35	8. Service Level Agreement	79	In case issues are not rectified to the complete satisfaction of Client, within a reasonable period of time defined in the RFP, the Client shall have the right to take appropriate remedial actions including liquidated damages, applicable penalties, or termination of the Contract.	Kindly elaborate the quantum and mechanism of calculation of liquidated damages?	As per RFP
36	7. Bid Opening and Proposal Evaluation Process	66	Shall be a company registered under the Companies Act, 2013 or the Companies Act, 1956 or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 _Shall be registered with GST Authorities in India _Should have their registered offices with legal presence in Mumbai Metropolitan Region.	On page 61 it is mentioned as follows "Below mentioned resources will be working from their own office on website redesign, development, and implementation. However, successful bidder shall deploy 3 senior software developers separately within 15 days from the issuance of LOA for operating and maintaining the existing website till the new website goes live." Would request relaxation of registered office with legal presence in MMR as long as the bidder is able to ensure the service levels required for smooth execution of the project.	As per RFP

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
38	9.2. Successful bidder's Technical and Functional Compliance	111	SIEM Service	SIEM service should also consider incorporating the following features: 1. The solution must support direct Cloud to Cloud collection, without need for a collection agent when collecting from a cloud or API based source. 2. The solution must support collection from on premises data sources and cloud-based sources. 3. The platform must have an on-premises log collector which can run on a variety of platforms, including windows and Linux. 4. The solution should be able to connect to and collect from Amazon S3 Buckets, Google Cloud Storage (GCS) and Microsoft Azure Blob Storage, directly, when provided authentication credentials. 5. The vendor must supply a container image for the log collectors, for flexibility and running in a dockized environment. 6. There should be a possibility to match and filter out certain	As per RFP

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
				log messages at the log collector. 7. The solution should provide an ingestion API so that data can be pushed directly without needing a collector. 8. The solution should have a comprehensive enrichment pipeline which enriches the raw log information with additional organizational context. 9. The solution should have a robust, comprehensive, and extensible data model for normalization. 10. The solution should support creating customized key value pairs, into which data can be normalized. 11. The solution should attempt to automatically enrich a log containing a given hash value with other possible hash values using data from external sources. 12. There should be a possibility to request that data is re-parsed, for example to apply a change to a parser retroactively against historical log data. 13. The solution	

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
				should store the raw log message in its original format along with the enriched and normalized data. 14. The solution should keep the last 12 months of collected data online in hot storage available for fast search. 15. The solution should make the data available to be queried using standard SQL expressions if required. 16. The solution should support writing collected data to a Pub/Subtopic. 17. The solution should support structured and unstructured searching. 18. It should be possible to search raw logs with a regex string. 19. It should be possible to search raw unparsed logs. 20. The solution should be able to return results for searches against IP addresses, file hashes, domains, or usernames in seconds. 21. The solution should have different	

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
				views based on the type of artifact being searched. 22. The solution should support structured searching with logical operators, i.e AND, OR, NOT. 23. The solution should include an advanced detection and correlation engine. 24. The detection engine should support running rules retroactively. It should be possible to run newly created rules back on historical logs. 25. The solution should support writing detection rules as code and enabling these rules via API request. 26. The solution must support correlation including detection of events that do not exist. For example, detecting a new account made, but the account not being logged into within 1 hour. 27. It must be possible to return values that are calculated as part of the detection. 28. It must be possible to define a risk score on an individual detection	

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
				rule basis. 29. The solution must include an IDE for creating new detection rules. This IDE should support versioning and the ability for multiple users to fork rules and make changes. 30. The detection engine should have a proven track record at operating at a huge scale on big data loads. 31. The solution should be able to check indicators of compromise (IOC's) against 12 months' worth of history automatically upon ingestion of a new IOC. 32. The solution should come with out-of-the box threat intelligence content. 33. Included threat intelligence must be able to be used within threat detection rules. 34. The solution should come with Use cases and detection content which are maintained by the vendor. 35. It must be possible to run a simple search - for example looking up a username or an IP address without needing to learn a	

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
				query language. 36. The solution should have a built-in capability to detect if a domain is common or uncommon within the environment. 37. The solution should have custom views for users, assets and domains. 38. The solution must have an extensible way to create new dashboards and reports. 39. The solution must make it simple to filter large datasets down using filtering options after a search has been completed. 40. The solution should be a Software-as-a-service (SaaS) cloud-based solution. 41. The provider should handle the scaling, uptime and back-end operations to maintain and update the solution. 42. The solution must support integration with a third-party identity provider and SSO. 43. Software updates including features should be automatically delivered. 44. It should be	

No.	Section No.	Page No.	Content of RFP Requiring Clarification	Change/Clarification Requested	Response
				possible to create our own parsers. 45. It should be possible for the customer to provision accounts and access to the platform. 46. The solution must be tested and proven to work at petabyte scale. 47. The solution should be extensible and provide API endpoint(s) for all major functionalities and capabilities. 48. The solution must support collection and integration of common security products on the market.	

for Panicker

Systems Manager

CITY AND INDUSTRIAL DEVELOPMENT CORPORATION OF MAHARASHTRA LIMITED

(Government of Maharashtra Undertaking)

Request for Proposal for Selection of Service Provider for Cloud Infrastructure and Website Redesign and Development for CIDCO

CIDCO Bhavan, CBD-Belapur, Navi Mumbai-400614

Ref No.: 05/CIDCO/SD/SM/2023-24/ Corrigendum-2

CIDCO Limited
Systems Manager,
Systems Department
First Floor, CIDCO Bhavan
CBD Belapur, Navi Mumbai - 400 614
Contact number: 022-67918699
Fax: 022-67918166

Amendment of the RFP to be read as under:

NIB & Bidding Schedule

Bidding Schedule

Sr. No.	Critical Dates	(DD.MM.YYYY / Hrs. Mins.)
1.	Publishing Date	31.10.2023/17.00 Hrs.
2.	Document Download / Sale Start Date	31.10.2023/17.01 Hrs.
3.	Document Sale End Date	28.11.2023/17.00 Hrs.
4.	Bid Submission Start Date	31.10.2023/17.01 Hrs.
5.	Bid Submission End Date	28.11.2023/17.00 Hrs.
6.	Technical Bid Opening Date	29.11.2023/15.00 Hrs.

Sd/

Systems Manager