Expression of Interest (EoI)

EoI No.: EOT/COM/20-21/00046 Dated: 17-12-2020

Empanelment of Service Providers for Providing Cloud Services

Issued by:
West Bengal Electronics Industry Development Corporation Limited (WBEIDC),
(A Govt. of West Bengal Undertaking)
Webel Bhavan, Block-EP & GP, Sector-V,
Salt Lake, Bidhan Nagar,
Kolkata: -700091

Content

Expression of Interest

EoI No.: EOT/COM/20-21/00046 Dated: 17-12-2020

West Bengal Electronics Industry Development Corporation Limited (WBEIDCL) invites e-tender for the work mentioned in the Table1. E-Tenders are invited from reputed, experienced and financially sound Cloud Service Providers (CSP) having a valid MeitY, GoI empanelment or authorized partners of such CSPs for empanelment as Cloud Service Providers hereinafter refereed as Managed Service Provider (MSP). Submission of bid should be through electronic bidding process.

Table 1

Brief Description of Work	Tender Document Money (Rs) [Non-refundable] (Online)	Earnest Money Deposit (EMD) (Rs) [Refundable] (Online)	Last Date and Time of Bid Submission (Online)	Bid Opening Date and Time (Online)
Empanelment of Service providers for providing Cloud Services	INR 10,000/-	INR 1,00,000/-	31/12/2020 12:00 PM	04/01/2021 3:00 PM

a) Intending bidders to download the tender documents from the website https://wbtenders.gov.in directly.

b) The Bidder shall pay Tender Document Fee of INR 10,000/-and EMD of INR 1,00,000/- through net banking or through RTGS/NEFT in the portal of the website: https://wbtenders.gov.in as per G.O 3975-F(Y) dated 28th July 2016 issued by Finance Department, Govt. of West Bengal. For details regarding payment procedure & guideline on the same, bidders are advised to follow the mentioned order and portal.

c) Digitally signed Technical Bid and Financial Bid, to be submitted through the website https://wbtenders.gov.in

d) Submission of the Bid should be done as per the stated time schedule mentioned in "IMPORTANT DATES & INFORMATIONS" section of the RFP.

e) The Financial Bid of the prospective bidder will be considered only if the Technical Bid is found qualified by the 'Tender Evaluation Committee'. The decision of the 'Tender Evaluation Committee' will be final and absolute in this respect.

f) The Committee reserves the right to accept or reject the Tender with intimation to the Bidder/Participant/Applicant

The timelines for the EoI are mentioned in the Table below:

"IMPORTANT DATES & INFORMATIONS"

1.	EoI No. & Date	**EoI No.: EOT/COM/20-21/00046 Dated:** 17-12-2020
2.	Tender issuing entity	West Bengal Electronics Industry Development Corporation (WBEIDC) Limited
3.	Date of uploading EoI	17-12-2020
4.	Documents download start date (Online)	17-12-2020
5.	Last date & time for sending queries	22-12-2020
6.	Pre Bid Meeting date & Time(Online through MS Teams	Click Here to Join Pre Bid Meeting(MS Teams) 23-12-2020 12:00 PM to 1:00 PM
7.	Last date & time of Bid Submission	31-12-2020 12:00 PM
8.	Date & time of Bid Opening	04-01-2021 3:00 PM
9.	Venue of Bid Submission & Bid Opening	ONLINE
10.	WBEIDCL Contact Person for any Further clarifications	Wing Commander Pratul Show (Retired) G.M.(Commercial) E-Mail: pratul.show@webel-india.com

Table 2: Description of the work and timelines

A. Instruction to Bidders

a. Intending bidders may download the EoI document directly from the website https://wbtenders.gov.in.

b. Each bidder needs to obtain a Class-II or Class-III Digital Signature Certificate (DSC) for submission of EoI from the approved service providers on payment of requisite amount.

c. The digitally signed EoI response should be submitted in the website https://wbtenders.gov.in

d. Submission of EoI response will be done as per time schedule stated mentioned in the Table 1 of this document.

e. Limited tendering will be done among the qualified bidders evaluated by the EoI evaluation committee of WBEIDC to identify the MSP/CSP for their individual project.

f. The list of qualified bidders will be displayed in the website https://wbtenders.gov.in and notified to each successful bidder.
g. For any queries regarding this EoI, please contact with WBEIDC Limited contact persons as mentioned in the Table 1 of this document on or before last date of submission of queries. No queries will be entertained after this timeframe.
h. EoI responses are to be submitted online to the website before the prescribed date & time using the Digital Signature Certificate (DSC). Virus scanned and duly digitally signed copies of the documents are to be uploaded.

EoI response should contain:

- ✓ This EoI document, with all pages signed by the authorized signatory
- ✓ Covering letter (as per Annexure-I)
- ✓ General information of the bidder (as per Annexure-II)
- ✓ Financial capabilities of the bidder (as per Annexure-III)
- ✓ Credentials of the bidder along with relevant work orders, agreements and completion certificates
- ✓ The details of the project executed as per format mentioned in Annexure-IV and Work Order copies along with project completion certificates from the customers duly attested.
- ✓ Undertaking on Legal Compliance (as per Annexure- V)
- ✓ Understanding and technical write-up on scope of work and approach & methodology.
- ✓ Valid scanned copies of the following documents:
  - Certificate of Incorporation,
  - Power of attorney establishing the authorized signatory (mandatory for partnership firms)
  - Audited Balance Sheets and Profit & Loss Statements for the Financial Years 2017-2018, 2018-2019 and 2019-2020

B. Eligibility Criteria

- The bidder must possess the requisite prior experience, financial strength and technical capability in providing the services necessary to meet the requirements as described in the EoI document. The Bidder is required to meet all eligibility criteria mentioned below in order to qualify for empanelment.

- The bidder can be a CSP or an authorized partner of the CSP. In case of an authorized partner, the CSP can authorize bidder for the purpose of this EoI.

a. For Managed Service Provider (MSP)

#	Basic Requirement	Specific Requirements	Documents Required to be submitted
1	Financial Strength	• The bidder, as a single legal entity or its holding company, must have average annual turnover of minimum INR 1 Crores during the last three financial years (2017-18, 2018-19 and 2019-20). • The firm must have been a profit-making organization for the last three financial years (FY 2017-2018, 2018-2019 and 2019-2020).	• Audited financial statement for last three financial years along with CA certificate specifying the turnover.
2	Project experience	• The bidder should have undertaken at least one (1 no.) project of minimum value of INR 30 Lakhs involving cloud computing services Or • The bidder should have undertaken at least Two (2 nos.) project of minimum value of INR 15 Lakhs each involving cloud computing services Or • The bidder should have undertaken at least Three (3 nos.) project of minimum value of INR 10 Lakhs each involving cloud computing services within the last three financial years (FY 2016-17, 2017-18, 2018-19) from any Govt. Department / Quasi Govt. Dept. / PSU / Board / Council/ Large corporate or similar organization.	• Copy of client certification, work order, completion certificate or extract from the contract mentioning scope of work.

3	Letter of Authorization	• If the bidder is an authorized partner of a CSP which is empaneled with MeitY, the eligibility criteria shall provide an Authorization Certificate from a MeitY empaneled CSP which states clearly that the bidder has been authorized to participate in this bid.	• Authorization Certificate from as per Annexure- VI
4a	Legal Entity	• The bidder should have existence in India for last five (5) years at the end of 31st March 2020. • The bidder shall be solvent at the date of bidding	• Certificates of incorporation for Company/ Partnership Deed / Proprietorship firm self-declaration • Certificate from Statutory auditor / Chartered Accountant for existence of firm for last five years along with last three years Balance Sheet.
4b	Other legal documents	• Trade License • GST Certificate • Income Tax Return (Latest 5 years) • Copy of PAN • Articles of Association/ Company Registration (depending on company type)	• Copy of the valid documents
4c	Other legal documents	• The responding firm must not be blacklisted by any Government Department, Ministry or Agency in any country for breach of ethical conduct or fraudulent practices during the last three years.	• The bidder must provide self- declaration in the company's letter head (as per Annexure-VII)

5	Power of Attorney	• The bidder shall submit the Power of Attorney of Authorization for signing the bid in Rs.10.00 Non Judicial Stamp Paper.	• Scanned copy of Power of Attorney needs to be uploaded
6	Submission of EMD	• The Bidder shall pay EMD of Rs. <to be decided> through net banking or through RTGS/NEFT in the portal of the website: https://wbtenders.gov.in as per G.O 3975-F(Y) dated 28th July 2016 issued by Finance Department, Govt. of West Bengal. For details regarding payment procedure & guideline on the same, bidders are advised to follow the mentioned order and portal. The EMD should remain valid for a period of 45 days beyond the final bid validity period.	• Scanned copy of the EMD needs to be uploaded
7	Submission of Tender Document Fee	• Bidder should submit Tender Document Fee of <to be decided> in the form of Demand Draft from any Scheduled Bank in favour of WBEIDC LTD. payable at Kolkata.	• Scanned copy of tender fee needs to be uploaded

b. For Cloud Service Providers (CSP)

- CSP shall be Ministry of Electronics and Information Technology (MeitY) empaneled & STQC audited as per MeitY empanelment process as on the last date of submission of the bid.
- As per the MeitY Empanelment Criteria, CSP should be certified for ISO 27001, ISO 27017 and ISO 27018.
- CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1, SOC 2, SOC 3

#	Basic Requirement	Specific Requirements	Documents Required to be submitted
1	Power of Attorney	• The bidder shall submit the Power of Attorney of Authorization for signing the bid in Rs.10.00 Non Judicial Stamp Paper.	• Scanned copy of Power of Attorney needs to be uploaded
2	Submission of EMD	• The Bidder shall pay EMD of Rs. INR 1,00,000/- through net banking or through RTGS/NEFT in the portal of the website: https://wbtenders.gov.in as per G.O 3975-F(Y) dated 28th July 2016 issued by Finance Department, Govt. of West Bengal. For details regarding payment procedure & guideline on the same, bidders are advised to follow the mentioned order and portal.	• To be submitted online
3	Submission of Tender Document Fee	• Bidder should submit Tender Document Fee of Rs. INR 10,000/- through net banking or through RTGS/NEFT in the portal of the website: https://wbtenders.gov.in as per G.O 3975-F(Y) dated 28th July 2016 issued by Finance Department, Govt. of West Bengal. For details regarding payment procedure & guideline on the same, bidders are advised to follow the mentioned order and portal.	• To be submitted online

Note:

- In absence of any of the above, the bid will be treated as non-responsive and hence shall be rejected.
- The duration of the empanelment is for 3 years from the date of awarding of Letter of Empanelment and can be renewed for a further period of 2 years (1-year extension at a time) based on the evaluation of performance on same terms and conditions.

C. General Terms & Conditions

i. Schedule of the EoI Document

a. The EoI response must be received by WBEIDC Limited before the scheduled time.
b. Beyond scheduled submission time, no response will be accepted by WBEIDC Limited and returned unopened to the Bidder.
c. WBEIDC Limited shall not be responsible for any delay or non-receipt of the EoI response. No further correspondence on the subject will be entertained.
d. The EoI Response submitted by fax, e-mail etc. shall not be considered. No correspondence will be entertained on this matter
e. WBEIDC Limited reserves the right to modify and amend any of the above-stipulated condition/criteria depending upon project priorities vis-à-vis urgent commitments.

ii. Clarification regarding EoI document

a. A prospective Bidder requiring any clarification about the EoI document and scope of work may contact the concerned person through e-mail/ letter as mentioned above.
b. No queries from the prospective Bidders will be entertained after the date & time mentioned in this document.
c. After opening of EoI responses, if tender committee feels, they may ask for supporting documents in respect of the claim of the bidder and the bidder must submit supporting document as well as written clarifications required by the committee within three days.

iii. Language of EoI

The EoI response submitted by the bidder should be in English language only. All the documents relating to the EoI (including brochures) supplied by the firm should also be in English, and the correspondence between the Bidder & WBEIDC Limited will be in English language only.

iv. Formats and Signing of EoI

The original EoI shall be neatly typed and shall be signed by an authorized signatory/ signatory on behalf of the Bidder. The authorization shall be provided by written Power of Attorney accompanying the EoI. The person or persons signing the EoI shall initial all pages of the EoI, except for unamended printed literature. The EoI shall contain no interlineations, erasure or overwriting. In order to correct

errors made by the Bidder, all corrections shall be done & initialed with date by the authorized signatory after striking out the original words completely.

D. Special Terms & Conditions

1. Preparation of EoI

EoI shall be submitted in accordance with the following instructions:

a. EoI shall be submitted in the prescribed forms. All signatures shall be in longhand. Where there is conflict between the words and the figures, the amount in words shall govern.
b. All notations must be in typed. No erasures or overwriting will be permitted.
c. EoI shall not contain any recapitulation of the work to be done. Alternative EoI will not be considered unless called for. No written, oral, electronic, telegraphic or telephonic EoIs for modifications will be acceptable.
d. EoIs shall be uploaded to the website as notified on or before the date and time set for the opening of EoIs in the Instruction to Bidder section.
e. EoIs subject to any conditions or stipulations imposed by the bidder are liable to be rejected.
f. Every page of the EoI document must be signed with date and company seal by the bidder. This is required to show that the bidder has accepted all the terms and conditions mentioned in this EoI document.

2. Opening of EoI

The EoIs shall be opened at the time set forth in the document. Bidders or their authorized representatives are invited to be present and to put their signatures on the records of EoI opening as each EoI is opened.

3. Acceptance of EoI

The acceptance of the EoI will rest with the accepting authority who is not bound to accept any EoI and reserves the right to reject in part or in full any or all EoI(s) received without assigning any reason thereof.

4. Awarding of contract

i. WBEIDC will use limited tendering for price discovery amongst the empaneled MSP/CSPs for their individual project. WBEIDC may use either LCBS or QCBS for awarding the contract for the respective individual project.

ii. The "Empaneled MSP/CSPs" will sign the contract with WBEIDCL within 15 working days of the release of notification and submission of fixed performance security. After signing of the contract, no variation in or modification of the terms of the contract shall be made except by mutual written amendment signed by both the parties.

E. Scope of Work

A. For Managed Service Provider (MSP)

I. <u>General</u>

a. The MSP shall be responsible for providing the required Cloud Services and Cloud Manage Service based on requirement and type of application.

b. The MSP shall provide inter-operability support with regards to available APIs, data portability etc. for the Government entities to utilize in case of change of existing cloud service provider, migration back to in-house infrastructure, shifting to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.

c. The MSP would be required to create and maintain a Helpdesk / telephonic number and email-based ticketing system that will resolve problems and answer queries related to the work order. The MSP shall provide the single point of contact for each client for any support request of the client on 24 x 7 x 365 basis.

d. The MSP through its CSP should provide all variants of cloud service – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

e. The MSP must be capable of providing complete service within 3 working days of placing the order.

f. Billing may be time based dynamic up to numbers of Cores, RAM usages or consumption-based billing.

g. It should be possible at any time to migrate from the Private Cloud environment to Government Cloud Infrastructure. The mechanism and technical requirements for achieving this should be well documented for above flexibility

h. The MSP on its own or through its CSP must have the following capabilities:

i. Per minute billing.
ii. Freedom to adopt new Platforms and / or upgrade of existing platforms in an uncomplicated manner.
iii. Hybrid Cloud.
iv. Intimation regarding availability of software updates.
v. Virtually unlimited storage with option to increase storage in real time without human intervention of the CSP.
vi. Active Directory support.
vii. Infrastructure as Code including post deployment scripting, service start-up and shut-down [based on tagging framework], etc.
viii. RESTful APIs for data access.
ix. Metered pricing for capacity, data transfer and/or requests at a granular level (for example, per gigabyte per month for storage, per gigabyte transfer per month for bandwidth, etc.).
x. Object-based cloud storage offering in general availability.
xi. Software-defined compute, storage and networking, with access to a web services API for these capabilities.
xii. Cloud software infrastructure services facilitating automated management, including, at minimum, monitoring, autoscaling services and database services.
xiii. A distributed, continuously available control panel supporting a hyperscale architecture.
xiv. Real-time provisioning for compute instances (small VM within a reasonable time) and a container service that can provision containers in seconds.
xv. The ability to securely extend the customer's data center network (expandable up to 32 vCPU) into the cloud environment

xvi. The ability to support multiple users and API keys, with role-based access control.

i. The MSP should offer a self-service portal which allows the client's IT admins to do the following activities without human intervention of CSP:
   i. Provision of infrastructure services in near-real time.
   ii. Set rules for auto scaling of infrastructure.
   iii. Auto-scaling the infrastructure in near-real time, any number of times during a day.

j. The MSP has to ensure that all software being offered with the client (other Government Departments) are genuine and comply to the licensing policy of the software OEM.

k. The MSP should provide support to user profile management – Support maintenance of user profiles and CRUD Operations (CREATE, READ, UPDATE, DELETE).

II. Disaster Recovery Services

a. The MSP on its own or through its CSP shall provide business continuity and disaster recovery services to meet the RPO and RTO as per the service levels.

b. The RPO should be less than or equal to 2 hours, RTO shall be less than or equal to 4 hours, key transaction data shall have RPO of 15 minutes.

c. In case the primary environment goes down, the CSP shall scale up the DR environment for the services to be delivered without any effect on the performance.

III. Migration Services

a. Migration Services are not a part of Cloud Managed Services and will have to be taken separately even if Cloud Managed Services have been opted. If the Client does not have expertise to migrate their existing applications to Cloud, the Client can procure the cloud migration services from the MSP

b. Application and Infrastructure Discovery & Portfolio Analysis:
   i. Formulate a baseline of the Client's technical environment including inventory of both applications and infrastructure. This should also include development/testing environments in addition to the production environment.

ii. Document the technical details of the applications including technical architecture, integration with external solutions, underlying technologies / platforms, and underlying software. For each of the applications, capture the logical and physical deployment architecture providing the details of various architectural components (e.g., load balancer, firewall).

iii. Identify the applications and their dependencies on other components and services. Create a dependency tree that highlights all the different parts of the applications and identify their upward and downstream dependencies to other applications.

c. Define To-Be and Security Architecture for Cloud

i. Estimate the resources required on cloud based on the application, current / anticipated server, storage configurations and workloads.

ii. Define the indicative or the minimum requirements need to be provided for each kind of environment (Development, QA, Training, Staging, and Production - as applicable for the project) that is planned on cloud.

iii. CSP should propose and, in consultation with the department, finalize the security architecture for the workloads being migrated to cloud.

iv. Define the logical architecture indicating the different compute, storage, network, security and monitoring services that will be provisioned for deploying the application on cloud.

IV. **Cloud Managed Services**

a. In case the Client, does not have capacity to manage the provisioned cloud services, the Client can procure the cloud managed services (e.g., provisioning, security configuration, monitoring) from the CSP through the MSP.

b. These services exclude Migration Services and Exit Management Services, which need to be procured separately by the Client.

c. The scope of Cloud Managed Services includes the following: -

i. Resource Management: Adequately size the necessary compute, storage and other cloud services required, building the redundancy into the architecture and load balancing to meet the service levels. Based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the

compute and storage as per the performance requirements of the solution. The scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits have to be changed) has to be carried out with prior approval by Department.

ii. Patch & Configuration Management (Remote OS Administration): Manage the instances of compute, storage, and network environments. This includes department-owned & installed operating systems and other system software deployed by the CSP.

iii. User Administration: Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks. Implement Multi-Factor Authentication (MFA).

iv. Security Administration: Configure, monitor and regularly review the security services / configurations for the workloads deployed on Cloud. Monitor the environment for unauthorized activity / access to the systems and conduct regular vulnerability scanning and penetration testing of the systems.

v. Monitoring Performance and Service Levels: 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.

vi. Backup (if procured by the Client): Configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases as per the policy finalized by Client. Restore from the backup where required.

vii. Training:

- In case the Client does not have skilled resources or expertise to migrate to cloud or manage the provisioned environment, the Client can procure Migration Services and/or Cloud Managed Services (e.g., provisioning, security configuration, monitoring) and / or Exit Management Services from the CSP.

- Provide training to the officials of the Client on request. The training may be provided online or offline as per the requirements of the Client. The infrastructure for the offline training will be provided by the Client.

viii. Support for third party audits: Enable the logs and monitoring as required to support for third party audits.

ix. Miscellaneous: Advise on optimal operational practices, recommend deployment architectures for cloud infrastructures, design and implement automated scaling processes, day-to-day and emergency procedures, deploy and monitor underlying cloud services, performance reporting and metrics, and ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.

x. Provide the regular reporting to the Client: Security assessment report with respect to security configuration gaps and possible improvements to the security and compliance of cloud services on a quarterly basis. In case any gaps / scope for improvement are identified, the same needs to be discussed with the Client and resolved in mutual consultation with the Client, either as fixed and hence no longer a gap or acceptable risk and hence no further action required.

V. Exit Management Services

a. These services are relevant at the end of the contract duration or in case of any mid-way termination of the contract or work order.

b. Exit Management Services is not a part of Cloud Managed Services and will have to be taken separately even if Cloud Managed Services have been opted. But if the Client does not have expertise in migrate their existing hosted applications from the cloud provided by the CSP to another cloud or another facility as deemed fit by the Client, the Client can procure the Exit Management Service from the CSP

c. The CSP shall provide necessary handholding support (for a maximum of 30 days) to assist in transition of the services from the existing CSP to Client or a replacement CSP. The handholding support includes migration of the Virtual Machines, data, content and any other assets to the new environment created by the Client or any Agency (on behalf of Client) on alternate CSPs offerings to enable

successful deployment and running of the applications / websites on the new infrastructure.

B. For Cloud Service Provider (CSP)

1. Cloud Services

   i. The CSP will be able to provide all types of Cloud Services Model viz, IaaS, Paas, SaaS offered using Public Cloud, Virtual Private Cloud and Government Community Model.

   ii. The CSP should provisioned VMs, Storage, Bandwidth dynamically (or on-demand) on a self-service mode or as requested.

   iii. The CSP has to provide access to the required cloud services for the Client to provision, migrate their workloads, configure security and manage the end-to-end operations.

   iv. The CSP shall share the best practices with the Client with respect to architecture for resource optimization, high availability, security, reliability and reducing the risk of data loss / corruption.

   v. The proposed cloud environment should provide flexibility to scale the environment horizontally by adding more Virtual Machines of the same/ different configuration to a load balanced pool. It should be possible to scale the solution horizontally at any time. It should be possible to automate this process of scaling up and down automatically.

   vi. The CSP is required to have IPv6 support.

2. Service Level Agreement Management

   i. CSP should provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime 99.75%, SLA measured at the VM level & SLA measured at the Storage Levels.

   ii. Service Availability (Measured as Total Uptime Hours/ Total Hours within the month) displayed as percentage of availability upto one tenth of a percent

   iii. Within a month of major outage occurrence resulting in greater than 1 hour of unscheduled downtime. Describe the outage including description of root cause and fix.

iv. Service provisioning and de-provisioning time (scale up and scale down) in near real time should be as per the SLA requirement of the Government Department. The provisioning and de-provisioning SLAs may differ for the different cloud deployment model.

v. CSP shall implement the monitoring system including any additional tools required for measuring and monitoring each of the service levels as per the SLA between the Government Department and the CSP.

3. Vertical Scalability: Scale-up and scale-down of resources

   i. Due care would be taken by the Client in deciding the resources and services needed for every requirement. However, the need for increasing or decreasing the resources and services cannot be ruled out. Accordingly, the Client(s) may scale-down the resources or scale-up the resources as per their requirement, subject to below mentioned clauses.

   ii. All resources can be scaled up or down without any restrictions. The charges for replaced resource would be paid till they have been used. Similarly, the charges for additional resources would also be payable from the time they are put into service as per the rates provided by the CSP or as revised from time to time.

   iii. An amendment to the work order shall be issued by the Client whenever scale-down or scale-up (including auto scaling) of resources takes place.

   iv. The invoices by the MSP/ CSP should clearly indicate such scaling of resources.

   v. The prices with the scaled-up or scaled-down resources would be reflected in all future invoices.

   vi. The resources and services hired for any single requirement would continue to be provided by the same Cloud Service Provider to whom the order was placed initially until the next revision of prices (downward or constant).

4. Security Requirements

   i. Security provisioned by CSP shall be for full infrastructure i.e. Cloud-DC and Cloud-DR.

ii. Disaster Recovery (DR) site should not be in the same premises and also in the same seismic zone as Data Center (DC) site. Both DR and DC sites must lie within India.

iii. CSPs shall conduct DR drill once in every six months, of operation wherein the Primary DC shall 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, there should be no/minimal data loss depending on the application requirements of the user department.

iv. Automated switchover/failover facilities (during DC failure & DR Drills) to be provided and ensured by the CSP. The switchback mechanism shall also be automated process and there should be No data loss

v. CSPs shall allow audits of all administrator activities performed by Government Department and allow Government Department to download copies of these logs in CSV or any other desired format.

vi. Cloud Platform should provide Edge-to-Edge security, visibility and carrier-class threat management and remediation against security hazards like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, botnets, etc. Also, shall provide protection against network issues such as traffic and routing instability.

vii. CSPs shall deploy and update commercial anti-malware tools , investigate incidents, and undertake remedial action necessary to restore servers and operating systems to operation.

viii. CSPs shall meet and comply with all GoI IT Security Policies and all applicable GoI standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.

ix. CSPs shall provide vulnerability scan reports from Web Application, Database, and Operating System Scans or the services for the Government Department to run the vulnerability scan. The scan results (that fall under the scope of the CSP) shall be managed and recorded in Plans of Action and mitigated by the CSP.

x. The CSPs shall be responsible for monitoring, reporting, notifications/alerts & incident management, backup storage, scheduling & retention, restoration, backup data protection, etc.

xi. CSPs shall provide a mechanism to carry out regular health check on Department provisioned cloud infrastructure and facilitate download of the health check report as per the frequency identified/set by the User Department.

xii. For all Incidents/ Issues with Severity 'Critical and High', the CSPs Incident Management Team shall be activated to provide resolution as per defined SLA's by the User Department and closure of the Incident. The teams shall be responsible to send an Incident Report on daily basis or as desired by User Department for all such Incidents to all the stake holders including designated officials by the department.

xiii. The CSPs shall provide a secure, dual factor / multi-factor method of remote access which allows the Government Department designated personnel (privileged users) the ability to perform duties on the hosted infrastructure.

xiv. CSPs shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Government Department (Client)

5. Role of Cloud Service Provider (CSP)

i. CSPs offer tools and services to help Clients meet their compute/storage requirements and security objectives. CSPs (in case of managed services) and / or Clients are responsible for provisioning, configuration management, monitoring performance, governance & compliance and resource optimization using the breadth of services provided by the CSP.

ii. Migrating to cloud creates a model of shared responsibility between the Client and the CSP. The operations and maintenance of the infrastructure including host operating system and virtualization layer down to the physical security of the facilities in which the service operates will be the responsibility of the CSP. The Client has the responsibility for the management of the guest operating system (including updates and security patches), other associated application

software, and the configuration and management of the security solutions provided by CSP such as security groups, host-based firewalls, host-based intrusion detection/prevention, encryption, and key management solutions. Deployment on cloud requires continuous monitoring and management by the client.

iii. The CSP in consultation with the Client will strive to optimize the provisioned resources by understanding the usage patterns and recommending termination of the under-utilized instances through continuous optimization. The CSP is required to give timely suggestions for achieving such optimizations.

iv. The CSP may also provide technical support to the Client regarding the possibilities of application re-engineering using advanced cloud features (e.g., auto-scaling, content delivery network) and additional PaaS services where possible to get further cost optimizations

Note:

- The above scope of work is indicative and shall be finalized based on actual requirement of user department.
- The CSP must implement all recommendation published time to time by MeitY/ CERT-In and other agencies of GoI within the specified time limit.
- The CSP must adhere to all the guidelines as specified by CERT-In (http://www.cert-in.org.in/)
- CSP also need to adhere to the all guidelines and acts published by Government of India.

F. Annexures

a. Annexure I: Covering Letter for submission of EoI

(To be submitted on the letterhead of the bidder)

(Date)

To,

General Manager (Commercial),

WBEIDC,

Webel Bhavan, Block-EP & GP, Sector-V,

Salt Lake, Bidhan Nagar,

Kolkata: 700091

Ref: EoI No **EOT/COM/20-21/00046 Dated: 17-12-2020**

Sub: Submission of EoI for "Empanelment of Service providers for providing Cloud Services"

Dear Sir/Madam,

We have examined the EoI document, we, the undersigned, herewith submit our EoI in response to your EoI no **EOT/COM/20-21/00046 Dated: 17-12-2020** for "Empanelment of Service providers for providing Cloud Services", in full conformity with the said EoI document.

i. We have read the provisions of the EoI document and confirm that these are acceptable to us. We further declare that additional conditions, variations, deviations, if any, found in our EoI shall not be given effect to.
ii. We agree to abide by this EoI, consisting of this letter, the detailed response to the EoI and all attachments, for a period of 180 days from the date of submission of the bid.
iii. We would like to declare that we are not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this assignment and we are not under a declaration of ineligibility for corrupt or fraudulent practices
iv. We would like to declare that there is no conflict of interest in the services that we will be providing under the terms and conditions of this EoI.

v. We hereby declare that all the information and statements made in this EoI are true and accept that any misrepresentation contained in it may lead to our disqualification.

vi. We understand you are not bound to shortlist / accept any EoI you receive

Sincerely,

Signature of Authorized Signatory and Seal of the bidder
Name:
Designation:
Date:

b. Annexure II: Details of the Responding Bidder

1.	Name of the company	
2.	Official address	
3.	Phone No. And Fax No.	
4.	Corporate Headquarters Address	
5.	Phone No. And Fax No.	
6.	Web Site Address	
7.	Details of Company's Registration (Please enclose copy of the company registration document)	
8.	Name of Registration Authority	
9.	Registration Number and Year of Registration	
10.	Company's Revenue for last 3 years (Year wise)	
11.	Company's net worth for the last year	

c. Annexure III: Financial Capability

FINANCIAL CAPABILITY

(EoI No. **EOT/COM/20-21/00046 Dated: 17-12-2020**

FINANCIAL INFORMATION

Sl. No.	Name of the Bidder	Turnover (Rs/Lakh)		
		2017-18	2018-19	2019-20
1				

d. Annexure IV: Details of Projects undertaken

Assignment Name:		
Location in India:	Duration of Assignment:	
Name of Client:	Total Project Value:	
Address of the Client:	Value of the services provided by the bidder:	
Start date:	Completion date:	No. of person-months of the assignment:
Narrative description of Project:		
Description of actual services provided:		

e. Annexure V: Undertaking on Legal Compliance

(To be submitted on the letterhead of the bidder)

(Date)

To,

General Manager (Commercial),

WBEIDC,

Webel Bhavan, Block-EP & GP, Sector-V,

Salt Lake, Bidhan Nagar,

Kolkata: 700091

Ref: EoI No **EOT/COM/20-21/00046 Dated: 17-12-2020**

Sub: Submission of EoI for "Empanelment of Service providers for providing Cloud Services"

Dear Sir/Madam,

I/We as Applicant do hereby comply to the IT Act 2000 (including 43A) and amendments thereof; meet ever evolving Security Guidelines specified by CERT-In, and meet any security requirements published (or to be published) by WBEIDC or any standards body setup / recognized by Government of India from time to time and notified to the CSP by WBEIDC as a mandatory standard.

We confirm that all the services acquired under this application document including data will be guaranteed to reside in India and there shall not be any legal frameworks outside Indian Law that will be applicable to the operation of the service (and therefore the information contained within it).

We hereby confirm to abide by all the rules and legal regulations as prescribed by MeitY and other authorities time to time. We also agreed to execute an agreement mentioning the terms and conditions for payment of work supported by us if such award placed on us.

Sincerely,

Signature of Authorized Signatory and Seal of the bidder

Name:

Designation:

Date:

f. Annexure VI: MeitY empaneled CSP Authorization Form

No. _____ dated _____

To,

General Manager (Commercial)

WBEIDC Ltd

Webel Bhavan

Block EP & GP, Sector-V

Salt Lake Electronics Complex

Kolkata-700091

Dear Sir:

Bid No. _____

CSP <<NAME OF THE CSP>> (hereafter "CSP") is pleased to support <<PARTNER NAME>> for the pursuit of the **EOT/COM/20-21/00046 Dated: 17-12-2020**.

I/We confirm that as on the date of this letter <<PARTNER NAME AND ADDRESS>>, has due authorization from us to use our cloud services for the purposes of the above referenced tender. Should <<PARTNER>> be awarded the contract resultant from the above referenced tender, CSP will support <<PARTNER>> with our commercially available cloud services in accordance with the then prevailing commercial terms and agreements.

Yours faithfully,

(Name):_____

(Name of MeitY empanelled CSP):_____

Note: This letter of authority should be on the letterhead of the CSP and should be signed by authorized signatory

g. Annexure VII - Undertaking for Non-Blacklisting

(Self-declaration for not being blacklisted by any Government Entity)

(To be submitted on the Letterhead of the MSP)

(Place)

(Date)

To,

General Manager (Commercial)

WBEIDC Ltd

Webel Bhavan

Block EP & GP, Sector-V

Salt Lake Electronics Complex

Kolkata-700091

Ref: EoI for "Empanelment of Service providers for providing Cloud Services". Ref: EoI No. **EOT/COM/20-21/00046 Dated: 17-12-2020**

Dear Sir,

In response to the above mentioned EoI I/We, _____, as _____ <Designation> of M/s_____, hereby declare that we are not blacklisted or ineligible to participate for bidding by any State/Central Government, Semi-Government or PSU.

Sincerely,

Signature of Authorized Signatory and Seal of the bidder

Name:

Designation: