



Bidding Document No : OC10000386/KAV dtd. 10.12.2020

Name of Work: Infrastructure Deployment for Integrated Project Data and Document Management Platform

Page 1 of 24

NOTICE INVITING TENDER



Bidding Document No : OC10000386/KAV dtd. 10.12.2020

Name of Work: Infrastructure Deployment for Integrated Project Data and Document Management Platform

Page 2 of 24

SALIENT DETAILS OF THE TENDER NOTICE

Two parts ONLINE bid (E-tender) offers are requested from competent bidders against the tender having salient features as mentioned below:

Name of Work:	Infrastructure Deployment for Integrated Project Data and Document Management Platform
Tender No. & Date :	OC10000386/KAV dtd. 10.12.2020
Bidding Document & subsequent addendum / Corrigendum (if any) available on Website for viewing & downloading	The complete document is available on CPP Portal. (https://eprocure.gov.in/)
Tender Publish Date / download start date / Bid Submission start date & time	10.12.2020 at 17.00 hrs
Pre-Bid Conference (Date & Time)	Not Applicable
Last date of on line EMD submission:	21.12.2020 at 11.00 hrs
Tender document download end date & time / Bid Submission end date & time	21.12.2020 at 11.00 hrs
Bid opening date & time (Technical Bid)*	22.12.2020 at 11.00 hrs
Contact Person for any query/ clarification	Ms. Kaveri Hazarika, Mgr (Project-Commercial), Email- kaveri.hazarika@nrl.co.in
Online Opening of Priced Bids of Techno-Commercially Accepted Bidders	On date & time to be intimated later on to techno-commercially acceptable & qualified bidders
Earnest Money Deposit (EMD)	Rs. 1,00,000.00 (Rupees One Lakh only).

Note :

- If identified dates as (*) above happens to be a declared holiday/closed day in NRL, activity shall be conducted on next working day at the same time.
- All amendments, time extension, clarifications, etc. will be uploaded as a Corrigendum in the websites only. Bidders should regularly visit the above website(s) to keep themselves updated.
- Request for extension received from any bidder with less than two working days prior to bid due date shall generally be ignored, since there will not be adequate time for consideration. Bidders shall submit the bid directly and in their own name without involving any intermediaries.
- The EMD must be submitted online on the portal of HDFC bank (Detail instructions at Appendix -A) and its receipt must be uploaded along with offer. If the EMD is not received along with the offer, offer shall not be considered for opening.
- MSE bidders are exempted from submission of EMD. MSE bidders are required to upload UAM or EM Part-II instead of the EMD deposit receipt.

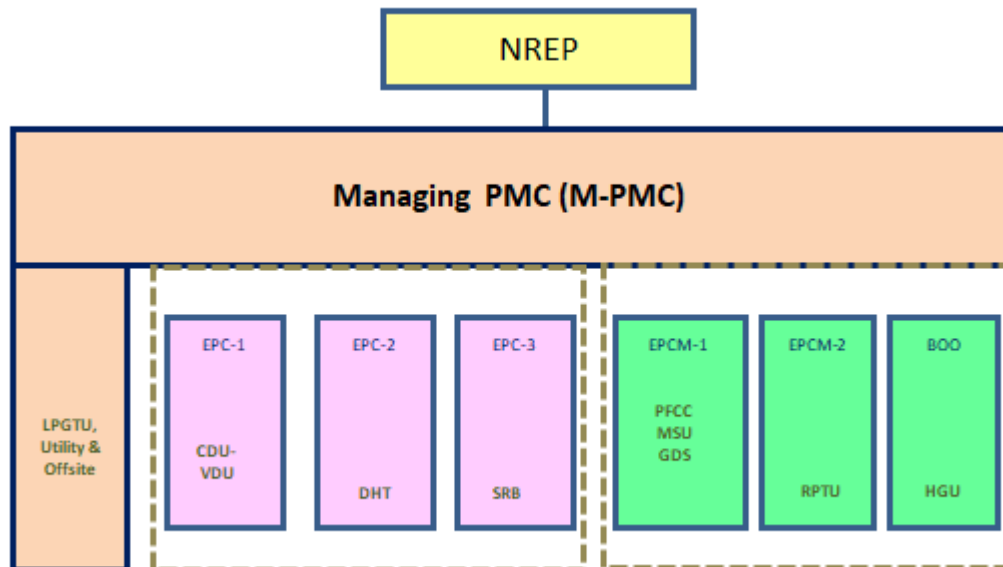


1.0 Introduction

Numaligarh Refinery Limited (NRL) presently operates a 3 MMTPA refinery in Golaghat District in the state of Assam. The refinery produces MS and HSD primarily conforming to BS-IV specifications by processing Assam Mix Crude.

Govt. of India approved capacity expansion of NRL from current 3 MMTPA to 9 MMTPA by installing new 6MMTPA refinery unit at its existing location in Assam. The Numaligarh Refinery Expansion Project (NREP) shall be executed with a project timeline of 48 months.

The Expansion Project is proposed to be executed in hybrid mode where a single Managing PMC (termed as M-PMC henceforth) will coordinate with 3 (three) EPC contractors and 2 (two) other EPCM consultants and 1 (one) BOO contractor. Figure below indicate the execution philosophy. Various Process Licensors being lined up for licensed units.



2.0 Brief Scope of Work:

This tender is for providing Cloud Services for Hosting and Managing the Integrated Engineering and Data management platform Project Collaboration Platform in NREP in cloud Consumption Model. NRL is implementing the Integrated Electronic Data & Document Management System (IEDDMS) integrating activities at MPMC/EPCM/EPC/Licensors and Owner (NRL) locations and the Platform will be hosted in cloud for access, collaboration of workflow management during project execution and later for operation and maintenance of Engineering Data. For details please refer the scope defined under Technical Section (Part –III).

3.0 Method of Bid Selection:

- i) Techno-commercial basis: Only bidders who are able to clear pre-qualification criteria (as mentioned in clause 4.1 below), will be evaluated further on technical parameters as listed in clause 4.2 below. The bidder must score minimum 75 marks out of 100 marks in the technical evaluation parameters to have their price bid opened.
- ii) Following the above evaluation, the offer of successful bidders shall be opened during priced bid.

4.0 Eligibility parameters and evaluation process:

The bidder(s) who satisfy the following qualification criteria shall be eligible to participate in the bid process. Offers received from the bidder(s) who do not fulfill all or any of the following qualification criteria shall not be considered for further evaluation.

**4.1 Pre-Qualification criteria:**

The bidder shall have to meet all of the below requirements to have the bid qualified and progress towards the technical evaluation process:

A. For Bidder			
Sl. No.	Parameters	Requirements	Supporting documentary evidences
1	Legal Entity / Registration of Company	The Bidder, as a single legal entity, must be registered in India and should have been in operations in India for a minimum of three (3) years by the date of opening of the bid.	1. Copy of certificates of incorporation Or 2. Registration Certificates
2	CSP Authorization	Bidder needs to be either CSP or MSP authorized by the proposed CSP to participate in the bid and shall provide the services only from that CSP under this bid.	Letter of support or Authorization Letter from the CSP to the Bidder for providing services for this particular Project.
3	Financial strength	Bidder should have a positive net worth in each of the last 3 years financial years (i.e. FY 2019-20, FY2018-19 & 2017-18). In case audited Figure of FY 19-20 is not available FY 2018-19 shall be considered Average Annual Turnover of the Bidder during last 03 financial years shall be minimum INR 0.50 Cr	1. Copy of the audited P&L and Balance Sheet or 2. Certificate from the Statutory auditor or Chartered Accountant
4	Work experience	Bidder should have experience of executing cloud implementation, managed services and cloud services consumption the last 05 years (ending on the last date of bid submission) as per the value given below: • 01 (one) project costing not less than INR. 0.85 Cr (including taxes) annual billing value. Or • 02 (two) projects costing not less than INR. 0.65 Cr each (including taxes) annual billing value. Or • 03 (three) projects costing not less than INR. 0.50 Cr each (including taxes) annual billing value.	1. Self-certificate from bidder's Country Head/CEO/CFO or authorized representative approved by the board – Format as per Appendix A) And 2. Copy of PO/WO and related invoices, and And 3. Certification from a Company Secretary or Chartered Account confirming the annualized billing value of work *If NRL desires further information to confirm the validity of the details, it may ask for additional details, including a reference call with concerned client of the bidder *** One year Billing details to be provided by bidder from respective CSP.

B. Requirement of CSP			
Sl. No.	Parameters	Requirements	Supporting documentary evidences
1	CSP's empanelment	CSP which is STQC (Standardization, Testing and Quality Certificate) audited and MeitY empanelled	1. Letter of Empanelment issued by MeitY
2	CSP's financial strength	The CSP must have an average annual turnover from operations of not less than Rs 500 crore for the last three consecutive financial years from Cloud related services in India. i.e. (FY 2017-18, 2018-19; FY 2019-20).- In case audited Figure of FY 19-20 is not available FY 2018-19 to be considered	1. Audited Financial statements by Chartered Accountant. or 2. Certificate from the Statutory auditor or Chartered Accountant
3	CSP's Quality certifications	CSP shall have the following third-party certifications: a. ISO 9001	1. Copy of Third Party Certificates



		b. ISO 27001 c. ISO 27017	
4	CSP's compliance to security, confidentiality and privacy of data	CSP should have accreditations of Service Organization Controls or SOC's (i.e. SOC 1, SOC 2 and SOC 3) relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles.	1. Self-declaration from the Country Head or authorized representative approved by the board of the CSP on their letter head for SOC 1, SOC 2 and SOC 3)

Notes:

- Both Cloud Service Providers (CSP) and Managed Service Providers (MSP) can participate in the tender.
- However the MSP shall have to be associated with a CSP during implementation of the Project and the MSP shall indicate the details of the CSP in technical bid. Once a CSP is finalized by MSP and details of which is furnished in technical bid, MSP cannot select another CSP during project implementation. An agreement/ MAF between MSP and CSP shall be submitted in Technical bid.
- Multiple bidders can propose the same CSP and a single bidder cannot propose multiple CSP. One bidder cannot bid with multiple CSPs.
- Joint venture and Consortium bidding is not allowed.
- Bidder will give details of their past experience along with documentary evidence as per **Annexure-III** to ITB enclosed herein.
- The value of past experience shall be adjusted at a simple rate of 07% for every completed year and thereafter at @0.58% for every completed month ending last day of the month proceeding the month in which last date of original bid submission falls.
- It is to be noted that experience as main contractor will only be taken cognizance of for the purpose of assessing qualifying criteria. However, authorized sub-contractors under principal contractors can also be considered provided their works completion certificate is issued by the client organization in case of job executed elsewhere under PSUs, limited companies, Government Departments, Quasi government and autonomous bodies. However, in case of sub-contractors under contractors engaged by NRL, the works completion certificate issued by the main contractor will also be acceptable provided the same is endorsed in original by Engineer-in-charge of NRL in terms of job description and value.
- Bidders are requested to confirm their valid GSTIN/UIN along with the Bid Document, with a copy of the relevant certificates. NRL at its discretion may not consider the bidder's offer for further evaluation if the GSTIN/UIN is not valid/ active. Any misinterpretation or misinformation with respect to GSTIN/UIN may attract penal action including putting the bidder on holiday / blacklisting as per rules in vogue at NRL.
- Bidder should not be under liquidation, court receivership or similar proceedings. Bidder shall submit a self- certificate to this effect.
- The bidder must submit copy (ies) financial documents – Trading and P/L account(s) along with the un-priced bid in support of the above criteria.
- In case audited balance sheets and profit and loss account for the immediate preceding financial year is not available for bid closing date up to 30th September, the Bidder has an option to submit the audited balance sheets and profit & loss account of the three previous years immediately prior to the last financial year. However, for bid closing date after 30th September, the bidder has to compulsorily submit the audited balance sheets and profit and loss account for the immediate three preceding financial years, for evaluation and his qualification with respect to financial criteria. In any case the date (i.e. the financial period closing date) of the immediate previous year's audited annual accounts should not be older than eighteen (18) months from the bid due date.
- Bids shall be liable for rejection without any notice to the bidder in case of non-submission of the following documents.
 - Income Tax / GST TDS Certificate from the client / proof of TDS, etc. for authentication of doing such jobs in case bidder submits experience of similar jobs under private limited company.
 - In case of the job is a part of composite work contract, then the bidder shall have to furnish documents certified by the client about the value for the portion of such "similar job".

**4.2 TECHNICAL CRITERIA:**

The bidders shall also be assessed on the following Technical Criteria, which carries a maximum of **#100 marks**. The bidder must score a minimum of **75 Marks** in this to have their price bid opened.

S. No.	Technical Parameters	Maximum Marks	Marks Distribution	Supporting evidences or medium
1.	Number of cloud certified engineers/architects on bidder's payroll	10	- Equal or more than #20 Architects/Engineers: 10 marks - Equal or more than #15 but less than #20 Architects/Engineers: 5 marks - Less than #15 Engineers/Architects: no marks	- Self-certification from Bidder's Country Head/CEO/CFO or authorized representative approved by the board And - Brief details (name, age, years of experience and qualification) of the Architects/Engineers & copy of their certificates
2.	Valid compliances certifications relevant to security, availability, Confidentiality, processing integrity, and privacy Trust Services principles	10	- ISO 27018: 5 marks - PCI DSS Level 1: 5 marks - None of the above: 0 marks	- Country Head or authorized representative approved by the board of the CSP And - Copy of the certificates
3.	Quality of Service offered in India.	30	- Technical proposal on proposed solution of a multi-site deployment, across geographically disparate sites, to ensure fault-tolerance with high availability between two physical sites. In case of failure, automated processes to shift application traffic to a secondary physical site: Maximum 10 marks. - Technical proposal on proposed solution with incremental block SSD storage with size of 10 GB or below: Maximum 10 marks. - Proposed CSP should have a point of presence or an edge location in Kolkata or Eastern India to deliver cached content: 10 marks	Bidder's technical proposal to include: - Solution architecture details and how it will meet stated requirements And - CSP's capabilities of the services with public reference able weblinks
4.	Platform Services for security and scalability	30	- Web Application Firewall: 6 marks - DDoS Protection Service: 6 marks - Security key management service: 6 marks - Auto-scalability of Compute: 6 marks - Auto-scalability of Storage: 6 marks	



5.	Industry Analyst Report: Presence of CSP in the latest Gartner Magic Quadrant for Cloud Infrastructure and Platform Services, published date September 2020	10	• Presence in Leader's Quadrant: 10 marks • Presence in other Quadrants: 5 marks • No presence: 0 marks	• Country Head /CEO /CFO or authorized representative approved by the board of the CSP on their letterhead And • Copy of the report or CSP's public reference able web links
6	CSP Console and monitoring	10	Demonstrate, at a high level, the CSP's console or publicly available offerings/resources: • Storage capabilities (block, object, archival and managed file system): Maximum 2 marks • Compute capabilities – ability to create a templated VM of 4 cores and 16GB RAM without Human intervention of CSP: 2 marks • Cloud managed databases: 2 marks • Self-provisioning console of the cloud platform (VMs of different configurations, Storage of different IOPS, etc.): Maximum 2 marks • Dashboard to monitor the cloud services like VMs and Storage Volumes: maximum 2 marks	Bidder to provide these details via detailed documents and screenshots in the technical proposal. During technical presentation: CSP/bidder shall login and demonstrate the native capabilities on offered cloud. Technical team of NRL will evaluate the native capabilities on live demo on CSP's cloud. In case the native capabilities are not available no marks will be assigned.
Grand Total		100		

SPECIAL NOTE TO THE BIDDERS:

Relaxation to MSE & Start-up agencies in line with Govt. circular is excluded for this tender However, relaxation of EMD as per MSE policy will be applicable. For further details please refer Annexure-III to SCC.



4.3 Documents required to be submitted in support of BQC

The response submitted by the bidder shall comprise the following documents:

- a) Bid Processing Fee and Earnest Money Deposit/Bid Security
- b) Bid Proposal form
- c) General Information
- d) Financial Capability with supporting documents
- e) Relevant Experience with supporting documents
- f) Self-Declaration
- g) All relevant Certification
- h) Proposal document containing a brief about the organization, its expertise and documentary evidences.
- i) Appendix C- Cloud Services Specifications and Requirements compliance
- j) Appendix B - Response to Pre-Qualification criteria for work experience

- 4.4** Bidder shall furnish documentary evidence by way of copies of work orders /Relevant pages of contracts, completion certificates from their clients, division of responsibilities for the work performed, completion certificate, MOU document/ commitment letters, Annual Reports containing audited balance sheets including Profit and Loss Accounts statement, in support of their fulfilling the qualification criteria.
- 4.5** In absence of such documents, NRL reserve the right to reject the Bid without making any reference to the Bidder or assigning any reason what-so-ever.
- 4.6** All documents furnished by the bidder in support of meeting the PQC (including MSE Certificate) shall be submitted/uploaded in a separate folder titled "Documents towards PQC", duly signed and stamped by the bidder (in case of proprietorship firm) or "Power of Attorney" holder in case of Partnership /firm/Company. Copy of such "Power of Attorney" shall also be furnished with the unpriced bid.
- 4.7** Bidders on "Holiday List of/debarred from business dealings by" NRL/Oil PSUs /MOP&NG shall not be considered for evaluation and ordering.
- 4.8** NRL decision on any matter regarding short listing of bidders shall be final.
- 4.9** **Submission of authentic documents is the prime responsibility of the Bidder. However, NRL reserves the right of getting the document cross verified, at their discretion from the document issuing authority. Bidder shall also facilitate such verification/ authentication of BQC documents and in case the documents remain unauthenticated till the given timeline, NRL reserves the right to reject such bid.**
- 4.10** NRL reserves the right to complete the evaluation based on the details furnished (without seeking any additional information) and / or in-house data, survey or otherwise.

5.0 Earnest Money Deposit:

- 5.1** Bidders are required to submit the EMD/Bid Security for the amount, online through the link: <https://nrl.procure247.com>.
- 5.2** Please note that EMD amount in online mode is only acceptable and no other mode i.e. offline or hard copy is not acceptable.
- 5.3** **In case non -submission of Bid Security / EMD as mentioned above shall be considered as non-responsive and such Bids shall be rejected.**
- 5.4** EMD exemption will be applicable only for Micro or Small Enterprises (MSEs) registered District Industries Centres or Khadi and Village Industries Commission or Khadi and Village Industries board or Coir Board or National Small Industries Corporation or Directorate of Handicrafts and Handloom or any other body specified by Ministry of Micro, Small and Medium Enterprises subject to:

- The unit being registered for the item tendered.



- Registration certificate being valid as on date of quotation.

6.0 Time Schedule:

Please refer Annexure II to SCC

7.0 Pre-Bid Conference: Not Applicable

8.0 Warranty/ Guarantee: Refer SCC.

9.0 Bid Validity: Validity of bid shall be 4 (Four) months from the final Bid Due Date.

10.0 TENDER DOCUMENT:

10.1 Tender documents should be downloaded from Central Public Procurement Portal <http://eprocure.gov.in/eprocure/app>. Aspiring Bidders/ Suppliers who have not enrolled/registered in e-procurement should enroll/register before participating, through the website <http://eprocure.gov.in/eprocure/app>. Bidders are advised to go through instructions provided as '**Instructions for online Bid Submission**' provided at Appendix A to Notice Inviting Tender.

10.2 Bidders can access tender documents from the website, fill them with all relevant information and submit the completed tender document into electronic tender on the website <http://eprocure.gov.in/eprocure/app>

10.3 Tenders and supporting documents should be uploaded through e-procurement portal only. Hard copy of the tender documents will not be accepted.

10.4 ***Corrigendum/addendum/extension (if any) pertaining to this tender will be published in the website only.***

10.5 Both Technical bid and Financial bid are to be submitted concurrently, duly digitally signed in the web site <http://eprocure.gov.in/eprocure/app>.

Online Bids are received only on CPPP Portal website <http://eprocure.gov.in/eprocure/app> on or before due date as indicated in the NIT. The bidder shall be at liberty to be present either in person or through an authorized representative at the time of opening of the Technical Bid. Price Bids of only those bidders shall be opened who are Techno-commercially qualified, at a time and place for which notice shall be given. The qualified bidders shall be at liberty to be present either in person or through an authorized representative at the time of opening of the Price Bids with the Bid Acknowledgement Receipt.

11.0 GENERAL:

11.1 The bidders shall give a declaration that the bidder shall not be under liquidation, court receivership or similar proceeding and their business is not banned by NRL, MOPNG or any OIL PSUs.

11.2 The bidders who are on Holiday / Negative list of NRL as on due date of submission of bid / during the process of evaluation of the Techno commercial bids, the offers of such bidders shall not be considered for bid opening / evaluation / Award. If the bidding document were issued inadvertently / downloaded from website, offers submitted by such bidders shall also be not considered for bid opening / evaluation/ award

11.3 NRL will not be responsible or liable for cost incurred in preparation, submission & delivery of bids, regardless of the conduct or outcome of the bidding process

11.4 In case any Bidder is found to be involved in cartel formation, his Bid will not be considered for evaluation / placement of order. Such Bidder will also be debarred from bidding in future

11.5 Canvassing in any form by the Bidder or by any other agency on their behalf may lead to disqualification of their Bid

11.6 Unsolicited clarifications to the offer and / or change in the prices during the validity period would render the bid liable for rejection

11.7 NRL reserves the right to reject any or all the bids received or annul the bidding process at any time



- 11.8** NRL reserves its right to allow Public Sector Enterprises (Central / State), purchase preference as admissible / applicable from time to time under the existing Govt. policy. NRL shall also follow the Public Procurement Policy on Procurement of Goods and services from Micro and Small Enterprises (MSEs) Order 2012.
- 11.9** Scanned copy of the Integrity Pact duly signed & stamped shall be uploaded along with the offer
- 11.10** For detailed specifications, terms and conditions and other details, refer complete Bidding Document
- 11.11** All questions and requests for clarifications or interpretations related to tender documents shall be addressed in writing to:

Ms. Kaveri Hazarika

Mgr (Project – Commercial)

Numaligarh Refinery Limited

Numaligarh – 785699, Dist- Golaghat, Assam

Email – kaveri.hazarika@nrl.co.in

Head (Proj-Commercial)

Numaligarh Refinery Limited

**Appendix-A****Instructions for Online Bid Submission**

As per the directives of Department of Expenditure, this tender document has been published on the Central Public Procurement Portal (URL: <https://eprocure.gov.in>). The bidders are required to submit soft copies of their bids electronically on the CPP Portal, using valid Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the CPP Portal, prepare their bids in accordance with the requirements and submitting their bids online on the CPP Portal.

More information useful for submitting online bids on the CPP Portal may be obtained at: <https://eprocure.gov.in/eprocure/app>.

REGISTRATION

- 1) Bidders are required to enroll on the e-Procurement module of the Central Public Procurement Portal (URL: <https://eprocure.gov.in/eprocure/app>) by clicking on the link "**Online Bidder Enrolment**" on the CPP Portal is free of charge.
- 2) As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.
- 3) Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPP Portal.
- 4) Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Class II or Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify / TCS / nCode / eMudhra etc.), with their profile.
- 5) Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSC's to others which may lead to misuse.
- 6) Bidder then logs in to the site through the secured log-in by entering their user ID / password and the password of the DSC / e-Token.

SEARCHING FOR TENDER DOCUMENTS

- 1) There are various search options built in the CPP Portal, to facilitate bidders to search active tenders by several parameters. These parameters could include Tender ID, organization name, location, date, value, etc. There is also an option of advanced search for tenders, wherein the bidders may combine a number of search parameters such as organization name, form of contract, location, date, other keywords etc. to search for a tender published on the CPP Portal.
- 2) Once the bidders have selected the tenders they are interested in, they may download the required documents / tender schedules. These tenders can be moved to the respective 'My Tenders' folder. This would enable the CPP Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.
- 3) The bidder should make a note of the unique Tender ID assigned to each tender, in case they want to obtain any clarification / help from the Helpdesk.

PREPARATION OF BIDS

- 1) Bidder should take into account any corrigendum published on the tender document before submitting their bids.
- 2) Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid.



- 3) Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF / XLS / RAR / DWF formats. Bid documents may be scanned with 100 dpi with black and white option.
- 4) To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use "My Space" area available to them to upload such documents. These documents may be directly submitted from the "My Space" area while submitting a bid, and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process.

SUBMISSION OF BIDS

- 1) Bidder should log into the site well in advance for bid submission so that he/she upload the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
- 2) The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document.
- 3) Bidder has to select the payment option as "offline" to pay the tender fee / EMD as applicable and enter details of the instrument.
- 4) **Bidder(s) must follow the following for submission of online EMD:**
 - User Manual for Bidders is available in NRL Website under <https://www.nrl.co.in> → Tenders → Tender Manual → EMD Online Deposit Manual (HDFC Bank Payment Portal)
 - Visit HDFC Bank Payment Portal URL: <https://nrl.procure247.com>
 - Click on 'Bidder Registration'
 - Bidder Registration Screen shall appear – Fill the mandatory details required and complete the process.
 - On successful submission of details in bidder registration form, bidder will get the system generated link to verify his/her email id and login to the website. Without verifying email id bidder may not be able to login to the system.
 - After successful email verification – please login with your user id and password
 - Bidder will receive system generate One Time Password (OTP) on their registered mobile number. In case not receiving of OTP please click Regenerate OTP and login.
 - After login Screen bidder can search the tenders and proceed for EMD payment.
 - Bidders' have to click on Payment Dashboard option available under Action tab
 - Payment Dashboard – Click on Pay to proceed further for the selection of payment mode.
 - Smart Hub – Bidders' can select the online payment and click on Pay to proceed further.
 - After click on Pay – Bidder will get an option for Cards and Net Banking. Bidders can select their preference and proceed further for the payment.
 - On successful payment bidder will receive system generated message on screen stating "EMD paid successfully"
 - Bidders' can also download the Payment receipt from Payment Dashboard.
 - Downloaded payment receipt – Bidders' can easily print the receipt and use it for their bidding purpose.
 - Since the HDFC Bank payment gateway is not under the CPPP, so the payment mode is mentioned as offline (BG) in the CPP portal. Bidder has to make a dummy entry in the EMD fields of CPPP by putting 'Transaction ID' (HDFC Bank payment receipt) as instrument no., payment date as issue date, any date as expiry date, and bank name as issuer details. Please upload the EMD payment receipt along with technical bid.
 - For any technical help, the bidders can contact HDFC Bank executive Mr. Tapan Desai at Mobile No: 8866287104 and email: tapan@tender247.com.

A receipt will be generated after successful payment (irrespective of the mode of payment). Bidder can take print out for onward submission with tender as well as save a soft copy of the receipt.

Foreign Bidders may submit the EMD wither in the form of crossed Demand Draft in favour of "Numaligarh Refinery Limited" payable at Numaligarh or Bank Guarantee (BG). BG shall be submitted from any Indian scheduled bank which includes



Indian branch of foreign bank recognized as scheduled bank by RBI. Bids without the requisite EMD as mentioned above shall be rejected.

There will be no waiver of EMD for Public Sector Undertaking of Central/State Government Undertakings. EMD shall be valid for a period of 08 (Eight) months from the final bid due date for submission of Bids.

- 1) Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the priced bid have been given as a standard BOQ format with the tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BOQ file, open it and complete the white colored (unprotected) cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BOQ file is found to be modified by the bidder, the bid will be rejected.
- 2) The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.
- 3) All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data. The data entered cannot be viewed by unauthorized persons until the time of bid opening. The confidentiality of the bids is maintained using the secured Socket Layer 128 bit encryption technology. Data storage encryption of sensitive fields is done
- 4) The uploaded tender documents become readable only after the tender opening by the authorized bid openers.
- 5) Upon the successful and timely submission of bids, the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.
- 6) The bid summary has to be printed and kept as an acknowledgement of the submission of the bid. This acknowledgement may be used as an entry pass for any bid opening meetings.

ASSISTANCE TO BIDDERS

- 1) Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.
- 2) Any queries relating to the process of online bid submission or queries relating to CPP Portal in general may be directed to the 24x7 CPP Portal Helpdesk. The contact number for the helpdesk is 1800-3070-2232.

3) For any assistance, please contact the following person:

Dhiraj Mohan Saikia, Phone No 03776 – 265774,

E mail: z_tender@nrl.co.in

Special Instructions to the Bidders for the e-submission of the bids online through e-Procurement Portal:

- Bidder should do Online Enrolment in this Portal using the option Click Here to enrol available in the Home Page. Then the Digital Signature enrolment has to be done with the e-token, after logging into the portal. The e-token may be obtained from one of the authorized Certifying Authorities such as eMudhraCA/GNFC/IDRBT /MTNLTrustline/SafeScript/TCS.
- Bidder then logs into the portal giving user id / password chosen during enrolment.
- The e-token that is registered should be used by the bidder and should not be misused by others.
- DSC once mapped to an account cannot be remapped to any other account. It can only be Inactivated.
- The Bidders can update well in advance, the documents such as certificates, purchase order details etc., under **My Documents** option and these can be selected as per tender requirements and then attached along with bid documents during bid submission. This will ensure lesser upload of bid documents.
- After downloading / getting the tender schedules, the Bidder should go through them carefully and then submit the documents as per the tender document, otherwise, the bid will be rejected.



- The BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevant columns, else the bidder is liable to be rejected for that tender. Bidders are allowed to enter the Bidder Name and Values only.
- If there are any clarifications, this may be obtained online through the e-Procurement Portal, or through the contact details given in the tender document. Bidder should take into account of the corrigendum published before submitting the bids online.
- Bidder, in advance, should prepare the bid documents to be submitted as indicated in the tender schedule and they should be in PDF/XLS/RAR/DWF formats. If there is more than one document, they can be clubbed together.
- Bidder should arrange for the EMD as specified in the tender.
- The bidder reads the terms and conditions and accepts the same to proceed further to submit the bids
- The bidder has to submit the tender document(s) online well in advance before the prescribed time to avoid any delay or problem during the bid submission process.
- There is no limit on the size of the file uploaded at the server end. However, the upload is decided on the Memory available at the Client System as well as the Network bandwidth available at the client side at that point of time. In order to reduce the file size, bidders are suggested to scan the documents in 75-100 DPI so that the clarity is maintained and also the size of file also gets reduced. This will help in quick uploading even at very low bandwidth speeds.
- It is important to note that, **the bidder has to Click on the Freeze Bid Button, to ensure that he/she completes the Bid Submission Process. Bids which are not Frozen are considered as Incomplete/Invalid bids and are not considered for evaluation purposes.**
- In case of Offline payments, the details of the Earnest Money Deposit(EMD) document submitted physically to the Department and the scanned copies furnished at the time of bid submission online should be the same otherwise the Tender will be summarily rejected
- The **Tender Inviting Authority (TIA)** will not be held responsible for any sort of delay or the difficulties faced during the submission of bids online by the bidders due to local issues.
- The bidder may submit the bid documents online mode only, through this portal. Offline documents will not be handled through this system.
- At the time of freezing the bid, the e-Procurement system will give a successful bid updating message after uploading all the bid documents submitted and then a bid summary will be shown with the bid no, date & time of submission of the bid with all other relevant details. The documents submitted by the bidders will be digitally signed using the e-token of the bidder and then submitted.
- After the bid submission, the bid summary has to be printed and kept as an acknowledgement as a token of the submission of the bid. The bid summary will act as a proof of bid submission for a tender floated and will also act as an entry point to participate in the bid opening event.
- Successful bid submission from the system means, the bids as uploaded by the bidder is received and stored in the system. System does not certify for its correctness.
- The bidder should see that the bid documents submitted should be free from virus and if the documents could not be opened, due to virus, during tender opening, the bid is liable to be rejected
- The time that is displayed from the server clock at the top of the tender Portal, will be valid for all actions of requesting bid submission, bid opening etc., in the e-Procurement portal. The Time followed in this portal is as per Indian Standard Time (IST) which is GMT+5:30. The bidders should adhere to this time during bid submission.
- All the data being entered by the bidders would be encrypted at the client end, and the software uses PKI encryption techniques to ensure the secrecy of the data. The data entered will not be viewable by unauthorized persons during bid submission and not viewable by any one until the time of bid opening. Overall, the submitted bid documents become readable only after the tender opening by the authorized individual.



- During transmission of bid document, the confidentiality of the bids is maintained since the data is transferred over secured Socket Layer (SSL) with 256 bit encryption technology. Data encryption of sensitive fields is also done.
- The bidders are requested to submit the bids through online e-Procurement system to the TIA well before the bid submission end date and time (**as per Server System Clock**).

**Appendix B****Response to Pre-Qualification criteria for work experience****On bidders letter head**

To,

Date:

<<Designation of Authority>>

<<Bid calling Agency>>

<<Address>>

Sl. No.	Item	Response
1	Client name	
2	Single point of contact from bidder's organisation to address any queries on this reference	Name: Designation Phone no.: Email:
3	Client profile and business description	
4	Contract Start date	
5	Contract Duration	
6	Overall contract value (in INR cr)	
7	Annualized billing details (in INR cr)	
6	Scope of services provided	
7	Client reference/reasonable proof (enclosed letters) – for client reference through tele-conference, please provide: a) Name of Person b) Designation in the organization c) Position in the project d) Contact number e) E-mail id	
8	Any additional information	

I/we hereby declare that the details furnished above are true and correct to the best of my/our knowledge and belief and I/we undertake to inform you of any changes therein, immediately. In case any of the above information is found to be false or untrue or misleading or misrepresenting, I/we am/are aware that I/we may be held liable for it and NRL has the right to reject the offer in full or part without assigning any reasons, whatsoever.

Authorized Signature {In full and initials with Seal}:

Name and Title of Signatory:

Name of Bidder (Firm/ Company's name): In the capacity of:

Address:

Contact information (phone and e-mail):

Date& Time:

Place: _

**Appendix – C****Cloud Services Specifications and Requirements****A. Networking:**

Sl. No.	Requirement	Description	Compliance(Y/N) /Remarks
1.	Multiple network interface/instance	Cloud service should be able to support multiple (primary and additional) network interfaces.	
2.	Multiple IP addresses/instance	Cloud service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network Interface.	
3.	Ability to move network interfaces and IPs between instances	Cloud service should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.	
4.	Enhanced networking support	Cloud service should support capabilities such as single root I/O virtualization for higher performance (packets per second), lower latency, and lower jitter.	
5.	Network traffic logging - Log traffic flows at network interfaces	Cloud service should support capturing information about the IP traffic going to and from network interfaces.	
6.	Auto-assigned public IP addresses	Cloud service should be able to automatically assign a public IP to the instances.	
7.	IP Protocol support	Cloud service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols.	
8.	Use any network CIDR, including RFC 1918	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.	
9.	Static public IP addresses	Cloud provider must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.	
10.	Auto-created default virtual private network	Cloud service should be able to create a default private network and subnet with instances launching into a default subnet receiving a public IP address and a private IP address.	
11.	Subnets within private network	Customer should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block.	
12.	Subnet level filtering (Network ACLs)	Cloud service should support subnet level filtering – Network ACLs that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.	
13.	Ingress filtering	Cloud service should support adding or removing rules applicable to inbound traffic (ingress) to instances.	



14.	Egress filtering	Cloud service should support adding or removing rules applicable to outbound traffic (egress) originating from instances.	
15.	Disable source/ destination checks on interfaces	Cloud service should support the ability to disable Source/destination check on network interfaces. By default, compute instances perform source/destination checks.	
16.	Configure proxy server (NAT instance) at network level	Cloud service should support NAT instances that can route traffic from internal-only instances to the Internet.	
17.	Site-to-site managed VPN service	Cloud service should support a hardware-based VPN connection between the cloud provider and customer data center.	
18.	Virtual Network Peering	Cloud service should support connecting two virtual networks to route traffic between them using private IP addresses.	
19.	Multiple VPN Connections per Virtual Network	Cloud service should support creating multiple VPN connections per virtual network	
20.	BGP for high availability and reliable failover	Cloud provider should support Border Gateway Protocol. BGP performs a robust liveness check on the IPsec tunnel and simplifies the failover procedure that is invoked when one VPN tunnel goes down.	
21.	Private connection to customer data centers	Cloud provider should support direct leased-line connections between cloud provider and a customer datacenter, office, or co-location environment, which in many cases can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.	
22.	DNS based global load balancing	Cloud service should support Load balancing of instances across multiple host servers.	
23.	Load balancing supports multiple routing methods	Cloud service should support multiple routing mechanism including round-robin, failover, sticky session etc.	
24.	Front-end Load Balancer	Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.	
25.	Back-end Load Balancer	Cloud service should support an internal load balancer that routes traffic to instances within private subnets.	
26.	Health checks - monitor the health and performance of application	Cloud service should support health checks to monitor the health and performance of resources.	
27.	Integration with Load Balancer	Cloud service should support integration with load balancer.	



28.	Low Latency	The CSP should be able to provide a 10GB network connectivity between the servers if required.	
-----	-------------	--	--

B. Storage- Block Storage:

Sl. No.	Requirement	Description	Compliance(Y/N) /Remarks
1.	Support for storage allocated as local disk to a single VM	Cloud provider should offer persistent block level storage volumes for use with compute instances.	
2.	Storage volumes > 1 TB	Cloud provider should offer block storage volumes greater than 1 TB in size.	
3.	SSD backed storage media	Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies.	
4.	Provisioned I/O support	Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.	
5.	Encryption using provider managed keys	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES- 256 cryptographic algorithm.	
6.	Encryption using customer managed keys	Cloud service should support encryption using customer managed keys.	
7.	Durable snapshots	Cloud service should support point-in- time snapshots. These snapshots should be incremental in nature.	
8.	Ability to easily share snapshots globally	Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data center migration, and disaster recovery.	
9.	Attach more than one compute instance to a single volume	Cloud service should support adding more than one compute instance to a single storage volume in R/W mode so that many users can access and share a common data source.	
10.	Consistent Input Output per second (IOPS)	Cloud service should support 3 IOPS/GB and maintain it consistently at scale	
11.	Annual Failure Rates <1%	Cloud service should be durable and support annual failure rates of less than 1%	

**C. Storage- Object Storage:**

Sl. No.	Requirement	Description	Compliance(Y/N) /Remarks
1.	Scalable object storage service	Cloud provider should offer secure, durable, highly scalable object storage for storing and retrieving any amount of data from the web.	
2.	Low cost archival storage with policy support	Cloud provider should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.	
3.	Support for Server-side Encryption	Cloud service should support encryption for data at rest using 256-bitAdvancedEncryption Standard(AES-256) encryption to encrypt your data.	
4.	Support for Server-Side Encryption with Customer- Provided Keys	Cloud service should support encryption using customer-provided keys. These keys should be used to manage both the encryption, as data is written to disks, and decryption, when data is accessed.	
5.	Support for Server- Side Encryption with a Key Management Service	Cloud service should support encryption using a Key Management Service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly.	
6.	Object lifecycle management	Cloud Service should support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation/initial storage to deletion.	
7.	Data Locality	Cloud provider should provide a strong regional isolation, so that objects stored in a region never leave the region unless customer explicitly transfers them to another region.	
8.	Object change notification	Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).	
9.	High-scale static web site hosting	Cloud service should be able to host a website that uses client-side technologies (such as HTML, CSS, and JavaScript) and does not require server-side technologies (such as PHP and ASP.NET).	
10.	Object Versioning	Cloud Service should support versioning, where multiple versions of an object can be kept in one bucket. Versioning protects against unintended overwrites and deletions.	
11.	Flexible access-control mechanisms	Cloud service should support flexible access- control policies to manage permissions for objects	



12.	Audit logs	Cloud service should be able to provide audit logs on storage buckets including details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code.	
13.	Multi-factor delete	Cloud service should support multi-factor delete as an additional security option for storage buckets	
14.	Lower Durability offering	Cloud service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy.	
15.	Parallel, multipart upload	Cloud service should allow uploading a single object as a set of parts where each part is a contiguous portion of the object's data and these object parts can be uploaded independently and in any order.	
16.	CDN option for users	Cloud provider should offer a service to speed up distribution of static and dynamic web content.	
17.	Strong Consistency	Cloud service should support read-after-write consistency for PUT operations for new objects.	
18.	Storage gateway appliance for automated enterprise backups	Cloud provider should offer a storage gateway appliance for seamlessly storing on-premises data to the cloud.	
19.	Accept large data loads through shipped physical media	Cloud provider should support moving large amounts of data into the cloud by bypassing the internet.	
20.	Deliver large data exports through shipped physical media	Cloud provider should support moving large amounts of data out of the cloud by bypassing the internet.	
21.	Availability	For Object Storage, Geo-Redundant Storage should be offered which is designed for 99.99% availability and 99.999999999% durability.	

**D. Security and Administration:**

Sl. No.	Requirement	Description	Compliance(Y/N) /Remarks
1.	Control access to your cloud resources at a granular level	Cloud provider should offer fine- grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device.	
2.	Utilize multi-factor authentication when accessing cloud resources	Cloud service should support multi- factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.	
3.	Identify when an access key was last used to rotate old keys and remove inactive users	Cloud service should support reporting a user's access keys last use details.	
4.	Policy Simulator to test policies before committing to production	Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production.	
5.	Policy validation to ensure policies match intentions	Cloud service should support a policy validator to automatically examine non-compliant access control policies.	
6.	Directory as a service	Cloud provider should support setting up a stand-alone directory in the cloud or connecting cloud resources with existing on- premises Microsoft Active Directory.	
7.	User and Group management	Cloud service should support features such as user and group management.	
8.	Integration with your existing on- premises Active Directory	Cloud service should integrate with existing on-premise Active Directory.	
9.	Self-service password reset for cloud users	Cloud service should allow users to reset their password in a self- service manner.	
10.	Dedicated, hardware security module (HSM) appliance	Cloud provider should offer dedicated HSM modules. A hardware security module (HSM) is a hardware appliance that provides secure key storage and cryptographic operations within a tamper-resistant hardware module.	
11.	Managed service to create and control the encryption keys used to encrypt your data	Cloud provider should offer a service to create and control the encryption keys used to encrypt user data.	



12.	Audit of all action on keys	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.	
13.	Key Durability	Cloud service should support durability of keys, including storing multiple copies to ensure keys are available when needed.	
14.	Web service to record API calls and deliver log files	Cloud provider should offer a service to record history of API calls and related events for a user account.	
15.	Receive notification of API activity	Cloud service should support notifications when new log files are available.	
16.	Durable and inexpensive log file storage	Cloud service should support storing log files in a durable and inexpensive storage solution.	
17.	Choice of partner solution	Cloud service should support a variety of 3rd party solutions.	
18.	Latency to deliver API activity history to a storage bucket	Cloud service should deliver API activity history within a Reasonable timeframe (<30 minutes) from the time API call is made.	
19.	Aggregation across multiple accounts and multiple Regions for ease of use	Cloud service should support receiving log files from multiple regions and accounts to a single location for ease of use.	
20.	Managed service for resource inventory, configuration history & change notifications	Cloud provider should offer a service that provides resource inventory, configuration history, and configuration change notifications to enable security and governance.	
21.	Automatically records a resource's configuration when it changes	Cloud service should automatically record a resource Configuration when it changes and make this information available.	
22.	Examine the configuration of your resources at any single point in the past	Customer should be able to obtain details of what a resource's configuration looked like at any point in the past using this cloud service.	
23.	Receive notification of a configuration change	Cloud service should notify every configuration change so customers can process these notifications programmatically.	
24.	Create and manage catalogue of pre-approved services for use	Cloud provider should offer the ability to create and manage catalogues of IT services that are approved for use.	

**E. Support:**

Sl. No.	Requirement	Description	Compliance(Y/N) /Remarks
1	Service Health Dashboard	Cloud provider should offer a dashboard that displays up-to-the- minute information on service availability across multiple regions.	
2	365-day service health dashboard and SLA history	Cloud provider should offer 365 days' worth of Service Health Dashboard (SHD) history.	
3	Service to compare resource usage to best practices	Cloud provider should offer a service acts like a customized cloud expert and helps provision resources by following best practices.	
4	Monitoring Tools	Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health.	
5	Governance and Compliance	Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines. Ability to choose from a set of pre-built rules based on common best practices or custom rules (e.g., ensure Storage volumes are encrypted, Compute instances are properly tagged, and Elastic IP addresses (EIPs) are attached to instances) and continuously monitor configuration changes to the cloud resources and provides a new dashboard to track compliance status.	
6	Audit Trail	Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing	

Bidder to provide public reference link /CSP certification for all the points mentioned above.

Sign and Seal of Bidders Authorized Representative