E-GOVERNANCE SERVICES INDIA LIMITED

*Tender Ref. No.: CSCSPV/Data Center/2024-25/003*

# TENDER DOCUMENT

# for

# Supply, Installation, Testing & Maintenance

# of

# Data Center Equipment

# {Server & Storage, Network Equipment and Software}

**CSC e-Governance Services India Limited**

**238, Okhla Industrial Estate, Phase III New Delhi-110020**

**Tel No. 011-49754975**

**Website: www.csc.gov.in**

# Table of Contents

# Introduction

CSC e-Governance Services India Limited hereinafter referred to as "CSC SPV" New Delhi inviting online bids under Two Stage Bidding System from Established/Reputed Agencies based in India through GeM - bidding process for Supply and Installation of Data center equipment {Server & Storage, HSM, Network Equipment and Software} at different locations Pune (Maharashtra), Noida (Uttar Pradesh) and Okhla (New Delhi) under the administrative control of O/o CSC SPV, New Delhi**.**

**Table – 1**

| Tender Ref. No. | Description | EMD |
|---|---|---|
| CSCSPV/Data Center/2024-25/002 | Supply, Installation, Migration & Maintenance of Data Center equipment {Server & Storage, HSM, Network Equipment and Software} | Rs. 250000/- (Rupees Two Lakhs Fifty Thousand Only) |

**Scanned copy of the same shall be uploaded by Seller in the online bid and hard copy of the same will have to be submitted directly to the Buyer within 5 days of the bid opening date (GeM terms & conditions).

Bidders can download the complete set of bidding document from GeM portal. Bidders have to submit the bids online by uploading all the required documents {Mentioned in RFP} through Gem portal.

| SN | Particulars | Date |
|---|---|---|
| 1 | Date of publication of Bid | 18/01/2025 |
| 2 | Last date for Submission of query, if any, regarding bid. | 20/01/2025 |
| 3 | Issue of responses to pre-bid queries, addendum/corrigendum, if required | 20/01/2025 |
| 4 | Bid Closing Date | 27/01/2025 by 6:00PM |
| 5 | Opening of technical Bid | To be informed through GeM to the Technically Qualified Bidders. |
| 6 | Opening of Financial Bid | Same as above |

Bids will be accepted through online mode only (GeM). Manual bids will not be accepted under any circumstances. CSCSPV reserves the right to accept or reject any quotation in full or part thereof without assigning any reasons thereof.

**Note**: Any bidder who fails to submit all required documents or who submits only a portion of them will be disqualified from the bidding process. **The quality of the scanned documents** should be checked before upload, **will lead to rejection**. Decision of CSC in this regard will be final.

## Disclaimer

This Bid is not an offer by the O/o CSC SPV, New Delhi but an invitation to receive offers from vendors/bidders. No contractual obligation whatsoever shall arise from the bidding process unless and until a formal contract is signed and executed by duly authorized Officers of the O/o CSCSPV New Delhi with the vendor/ bidder.

## Clarification of bidding documents

A prospective bidder requiring any clarification about the RFP & any query shall contact the service receiver in writing at the following e-mail address i.e.

Email: leepika.banga@csc.gov.in **and** technology@csccloud.in

The receiver will respond in writing (e-mail/website/GeM) to any request for clarification, provided that such a request is received well within the time specified for submission of queries. No queries will be responded to after this day.

## Bid for Supply, Installation & Maintenance

of Data Center equipment and Accessories at CSC e-Governance Services India Limited, Plot # 238, Okhla Industrial Area Phase – 3, New Delhi and CSC Data Center Pune (Maharashtra) and Noida (Uttar Pradesh).

### 1. GENERAL

Bids are hereby invited by CSC SPV from reputed and experienced Companies registered in India and having Minimum 10 years of experience in Supply, Installation & Maintenance of Data Center Grade Servers, Storage, Network and Cyber Security Devices. The Bidder have to submit the proof of the same (Work Completion Certificate, not more than 3 Years old from the date of tender opening)

### 2. PARTICULARS OF THE BID

**(a) EARNEST MONEY DEPOSIT (EMD):**

The Earnest Money Deposit (EMD) of Rs. 250000/- (Rupees Two Lakhs Fifty Thousand Only), (refundable without interest) shall accompany the Pre-qualification Bid of the Bidder in the form of bank guarantee the format specified on GeM portal failing which the bid shall be rejected summarily.

The EMD of Unsuccessful bidders shall be released after the work order is placed to the successful bidder.

**(b) PERFORMANCE SECURITY DEPOSIT:**

On receipt of the Letter of Acceptance of Bid from the O/o CSC SPV, the successful Bidder should give a Performance Bank Guarantee in the form of bank guarantee in favor of "CSC e-Governance Services India Limited" payable at New Delhi from any Nationalized Bank or from any Scheduled Bank, amounting to Ten (10%) Percentage of the total contract/PO value. Performance Bank Guarantee shall be released after twelve months from the end of the month of satisfactory completion of equipment deployment & the submission of Installation Report including the OEM warranty and license details of each component on the Company Letter Head.

**(c) ADDRESS OF THE OFFICES for DELIVERY & Deployment:**

I. Address details are mentioned in the Annexure-V

## 3. REQUEST FOR BID ON GEM:

The agencies/parties interested in responding to this RFP must submit their bids online using GeM portal (gem.gov.in) in the prescribed formats along with all necessary documents and information requested herein.

Financial bids for only those bidders will be opened who are declared qualified in Technical evaluation. The date and time for opening of financial bids shall be separately notified on GeM Portal (gem.gov.in.). O/o CSCSPV may seek any further clarification or documents as required.

All details regarding the subject RFP are available on websites: www.gem.gov.in. Any changes/modifications/corrigendum in connection with this RFP will be intimated through this website only. Prospective bidders are therefore requested to visit above mentioned websites regularly to keep themselves updated. O/o CSCSPV shall not be liable to send any individual information or issue a public notice.

### A. ELECTRONIC SUBMISSION OF BIDS:

1. Bids against this RFP shall be received only electronically through the GeM Portal of NIC (www.gem.gov.in). No bids shall be accepted in hard copy or in any other form.
2. For submission of e-bids, bidders are required to get themselves registered with gem.gov.in website.
3. The bid will be submitted online in two Electronic Envelop systems.
    a) Electronic Envelope No-I: - Eligibility documents & Technical Bid.
    b) Electronic Envelope No-II: - Commercial Bid.
4. The Earnest Money Deposit (EMD) is required to be submitted in the form of bank guarantee the format specified on GeM portal failing which the bid shall be rejected summarily.
5. Scanned copy of the same (i.e. point (4)) shall be uploaded by Seller in the online bid and original document of the same should have to be submitted directly to the Buyer within five (05) days of bid opening date (GeM terms & conditions).
6. Bids should be submitted online by downloading an excel file and same can be uploaded after filling the rates for items without any alterations/cuttings etc. Such cuttings/alteration etc. even if accompanied by signature shall be liable to be rejected on such grounds.
7. The Online bid can only be submitted after uploading following valid scanned documents (i.e. Envelope-I) related to eligibility conditions up to Last date and time of online submission/uploading of bid.
8. Validity of bid shall be for sixty (60) days from the date of opening of bid.
9. The bidding process will be accepted only through GeM portal. As bidders are invited through e-Bidding process, a physical copy of the bid document would not be available for sale. Bidder can upload documents in the form of PDF format and any other format as permissible by the GeM portal.

For any queries relating to the process of online bid submission or queries relating to GeM Portal (gem.gov.in), Bidder may contact GeM Helpdesk Mail: gem[at]gov[dot]in; Toll Free Numbers: 1800-419-3436;1800-102-3436.

10. All Bidders are requested to furnish an EMD of two lakh fifty thousand rupees.
11. The envelope containing the EMD and undertaking along with Covering Letter mentioning the details of Bidder Company on the company's Letter head should be sealed and super-scribed as "tender Name: As mentioned above" and submitted physically to O/o CSC SPV, New Delhi (Address: Plot # 238, Okhla Industrial Area, Phase – III, New Delhi - 110020). The O/o CSC SPV shall not be responsible if Bidder document not submitted to office or delay in delivery.
12. Bids for which EMD is not received in the prescribed manner shall be rejected summarily.
13. O/o CSC SPV shall not be responsible for non-receipt/non/delivery/delayed receipt of the EMD due to any reason whatsoever. EMD shall not carry any interest.
14. EMD shall not carry any interest and EMD of unsuccessful bidders shall be returned after Award of Contract to the Successful Bidder. EMD of the successful bidder shall remain with O/o CSC SPV, New Delhi and shall be returned without interest within a period of six months.
15. The bidders availing exemption under MSME / Startup as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) or are registered with the Central Purchase Organization or the concerned Ministry or Department or Startups (as defined by Department of Industrial Policy and Promotion) are required to submit documentary proof for claiming such exemption subject to meeting of quality & technical specifications. Relevant documentary proof should be submitted by the bidder for claiming such relaxation to the office before the closing date of bid.
16. The bidder has to submit the Board of Resolution on behalf of the officer who is signing the bid with all of his information.

**B. BID DETAILS:**

Bidders are required to furnish the rates including all taxes/GST etc., strictly in the prescribed Performa of Financial bid. The financial bid shall contain price only and no other documents shall be enclosed with the financial bid.

**C. ELIGIBILITY CRITERIA FOR OEM:**

a) The Bidder must be a company registered in India under the Indian Companies Act 1956/2013 with their registered office in India for the last Seven years as on 31.03.2024.

b) The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Ministry/Departments of Govt. of India/Central PSUs/ Nationalized Banks/State Govt. Departments Autonomous/Statutory Bodies/ Corporations in India. The Work Certificates from the actual client will have to be submitted online. The Work Certificate shouldn't be older than three years. from the date of the bid opening. Client's Complete Contact Details should be provided by Bidder.

c) The original equipment manufacturers/System Integrator shall preferably possess an Valid ISO Certificate for their establishment. A copy of the valid ISO Certificate shall be placed with the Technical Bid.

d) The intending Bidder, in case of Authorized Distributor of OEM / Authorized Dealer of OEM shall possess valid authorized Distributorship / Dealership license from Original Equipment Manufacturers who should have valid ISO Certificate and shall be engaged in regular manufacturing and supply of similar Servers, Storage & network equipment for the last five (03) years. The Bidder shall enclose a copy of the proof document in technical bid while submitting the bid.

e) The OEM/Bidder should have proven facilities for Engineering, manufacture, assembly, integration and testing of the equipment's and basic facilities with respect to space, Engineering, Personnel, Test equipment, Manufacture, Training, Repair, Service Center Supports for at least past five years in the country from where the proposed equipment are planned to be supplied. The certificates/Undertaking for the same will have to be submitted offline (The bidder will have to submit the proof of establishment for the facility in India.).

**f)** The Bidder should have Minimum staff of 10 Skilled Manpower who have experience in Data center management services including firewall configuration and management on their payroll {Undertaking with Staff details & Designation including their Mobile Number and E-Mail IDs}

**D. QUALIFYING CRITERIA FOR BIDDER:**

a) The yearly average turnover shall be Rupees fifteen Crores (Rs. 15,00,00,000/-) during the preceding three years from the similar work of Supply, Deployment of data center grade equipment {Firewall, Servers, Security & Network equipment}. CA certificate (based on audited financials) should be submitted.

b) At least One Work order should be minimum value of Rs.6.00 crores. Copy of the work order to be submitted. The Work Order Document should not be more than 3 Years old. from the date of Bid. OR Two Work Order with total value of 6 crores not older than 3 Years.

c) ITR details must be submitted by the bidder for the current last three years. (FY 22 – FY 24)

d) The certificates from the actual/existing client will have to be submitted. (Not more than 3 years old)

e) The bidder should have authorization, specific to this bid from respective OEM as per Annex-II.

f) The bidder shall have successfully completed similar work during the last three years. Work Completed Client Certificate and allocated Work Order furnish the detail of Data Center grade equipment has to be submit by the bidder.

g) The bidder must submit declaration regarding not being blacklisted by any Govt. institutions, not be insolvent, in receivership, bankrupt or being wound up, not have its

affairs administered by a court or a judicial officer, should not have its business activities suspended and must not be the subject of legal proceedings for any of aforesaid reasons.

The OEM/Bidders exempted under Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) or are registered with the Central Purchase Organization or the concerned Ministry or Department or Startups (as defined by Department of Industrial Policy and Promotion) are required to submit valid documentary proof for claiming such exemption subject to meeting of quality & technical specifications. Relevant valid documentary proof shall be submitted by the bidder for claiming such relaxation to the office before the closing date of bid. Non valid Document will lead to rejection of the bid.

The Office of CSCSPV reserves the right to verify the proof of having experience and expertise of the bidder in executing similar works and the bidder has to produce the proof thereof.

Similar Work means - "Supply, Installation, Upgradation & Commissioning of High-end Servers, Firewall, Data Center Security and Networking Components / Management Contract of Data Center." Bidder has to Submit the valid Artifact for the same as per the RFP Conditions.

**E. WARRANTY:**

a) All equipment required licenses and components shall be supplied with **Five (05) years on-site warranty & Support**. OEM backend support 24X7 should be included. If during the said guarantee/warranty period, the Goods are found not conforming to the requisite description and quality and/or not giving satisfactory performance or have deteriorated, and the decision of the buyer in that behalf shall be final and binding on the seller and the buyer shall be entitled to call upon the Seller to rectify and /or replace the Goods or such portion thereof as is found to be defective by the buyer within seven (07) days. Otherwise, the seller shall have to pay Rupees Ten Thousand (Rs. 10000/-) per week or part of week for failed equipment subject to a maximum often (15%) percent of equipment cost to the buyer as compensation. Buyer has the right to cancel the order w/o any financial implication on buyer in case the equipment found non satisfactory as per the RFP terms.

b) Equipment should be offered with all necessary hardware/software to comply with all the required/support features.

c) Five Year Back-to-back onsite warranty with respective OEMs for both Hardware and software included all required components. <u>The certificates/undertaking for the same will have to be submitted along with bid from respective OEM.</u>

d) OEM should have its service center in India. Service Center Details to be shared along with the address and contact no. of the person.

e) Bidder shall provide maintenance support after successful installation of the product. The on-site warranty obligations for a minimum period of five (05) years for Data Center

equipment from the date of deployment/Handover. CSC SPV offices should extend the benefits of periodical software patches/updates made by OEM on the system from time to time for equipment security/performance without any additional cost to O/o CSC SPV.

f) All the required Licenses & equipment should be in the name of CSC e-Governance Services India Limited only.

**F. SLA DURING WARRANTY PERIOD:**

a) After having been notified of the defects, service requirement during warranty period, seller has to complete the required Service, Rectification and replacement of defective part, within time limit of support provided with the hardware (24x7, 365 days}. If the Seller fails to complete service, rectification, replacement within defined time limit, a penalty of half (0.5%) percent of Unit Price of the product shall be charged as penalty for each week of delay from the seller & up to max. of ten (10%) percent of Unit Price of the product. Seller can deposit the penalty with the Buyer directly else the Buyer shall have a right to recover all such penalty amount from the Performance Bank Guarantee (PBG) or from the pending payment/invoices with CSC SPV.

b) During the warranty period, rectify and fix the defects of equipment at the delivered location in case any cost of required expert(s) and any other associated expenditure shall be borne by the bidder, without any financial implication on CSC SPV.

c) Any part or parts fail or proved defective within the on-site warranty period specified above, owing to defects in design, material or workmanship, the bidder shall have to replace them at the place of deployment without asking for any charges.

**G. PAYMENT CONDITIONS:**

a) 30% payment against delivery & specification acceptance of the equipment at the specified locations. {Delivery Challans, Document and Accepted Certificate by CSC SPV Officials}.

   a. Provided Devices and License Details in name of CSC SPV.
   b. Original Performance Bank Guarantee.
   c. Certificate of receipt of Goods in good condition from all the locations of O/o CSCSPV.

b) 60% payment against the deployment and acceptance, after the successful signed installation certificates from the assigned CSC SPV Representative at the specified locations. The following documents has to be submitted by the bidder along with the invoices:

   a. Certificate of receipt of Goods in good condition & installation certificate thereof from all locations of O/o CSCSPV.

**c)** 10% Payment will be released after 12 Months from the date of the first Invoice.
*Any deviation in the delivered items will impact to the balance payout.

**H. CONTRACT PERFORMANCE BANK GUARANTEE:**

a) On receipt of the Letter of Acceptance of Bid from the O/o CSCSPV, the successful Bidder should give a Performance Bank Guarantee in the form of DD/ Bank Guarantee in favour of "CSC e-Governance Services India Limited" payable at New Delhi from State Bank of India/any Nationalized Bank or from any Scheduled Bank, amounting to five (5%) percent of the total contract/PO value.

b) The successful bidder shall have to submit a Performance Bank Guarantee (PBG) within Ten (15) days from the date of issue of Letter of Acceptance (LOA). Extension of time for submission of PBG beyond Ten (15) days and up to twenty (25) days from the date of issue of LOA may be given in written by the Authority who is competent to sign the contract agreement. However, a penal interest of twelve (12%) percent per annum shall be charged for the delay beyond Twenty (25) days, i.e., from twenty first ($26^{th}$) day after the date of issue of LOA. In case the Bidder fails to submit the requisite PBG even after forty-five (45) days from the date of issue of LOA, the contract shall be terminated duly forfeiting EMD and other dues, if any payable against that contract. The failed Bidder shall be debarred from participating in a rebid for that work.

c) The Performance Bank Guarantee should be furnished by the successful Bidder after a letter of acceptance has been issued, but before signing of the agreement. The agreement should normally be signed within twenty (15) days after the issue of LOA and Performance Bank Guarantee should also be submitted within this time limit. The PBG will be returned only after 12 months of the said project.

**d)** **Performance Bank Guarantee shall be** released after twelve months from the end of the month of satisfactory completion of equipment deployment & the submission of Installation Report including the OEM warranty and license details.

e) Wherever the contracts are rescinded, the Performance Bank Guarantee shall be en- cashed and the balance work should be done separately.

f) The Performance Bank Guarantee should be valid for up to 24 months.

**I. Delivery:**

a) Delivery Timelines for required equipment other than HSM are 60 days at the given locations. Delivery Timelines for HSMs are 30 days at the given locations.

b) 20 days will be given for the designing, deployment, migration & acceptance testing.

c) Penalty regarding Delay in Supply: Any delay in supply of the equipment will invite a penalty @ half (0.5%) percent per week of the total work order value.

d) Delay in supply in part or specific part of the components will invite a penalty @ Twenty (20%) percent of the total cost of the part/s.

e) Delay of deployment will invite the penalty of 0.5% percent per week of the total work order value. In case of extra time required for the delivery or deployment the same will be approved by CSC SPV CTO/DY CTO/Management in written, valid reason for the delay has to be confirmed by Bidder/OEM.

f) The material shall be inspected on receipt at site (at every location as mentioned) and bidder shall be responsible for any damage during the in- transit of the required equipment mentioned in the RFP. CSC SPV will not dear any cost related to replacement of damaged equipment.

g) The bidder shall not arrange part shipments and/or trans-shipments without the permission of purchaser. The insurance cover including insuring the goods against the loss or damage incidental to manufacture or acquisition, transportation, storage and delivery, Installation & Commissioning shall be obtained by the bidder in his own name and not in the name of purchaser. The purchaser will as soon as possible but not later than thirty (30) days from the date of arrival of goods at destination shall notify the bidder of any loss or damage to the goods.

**J. Evaluation methodology:**

***a) Evaluation of Bid:***

The bidders are required to upload soft copies of the following documents for Technical Evaluation. If Bidders fail to upload soft copy of any of the Following document in technical Evaluation. Bidder will not be considered for financial evaluation and shall be treated as disqualified. Bidders should submit EMD; undertakings on judicial stamp papers (original documents) on or before closing date of bid for verification at the time of technical Evaluation.

i. Copy of PAN Card No and GSTIN No.
ii. Scanned copy of Demand Draft/Banker cheque submitted towards Earnest Money Deposit as mentioned in the technical bid or self-attested copy of MSME Registration certificate with the name of bidder or DPIIT certification for startups with the name of bidder.
iii. Copy of required Experience Certificate (work order and Satisfactory Completion Certificate).
iv. Proof of yearly average turnover shall be Rupees Fifteen crore (Rs. 15,00,00,000/-) during the preceding three (03) years. CA Certificate of the annual turnover (as per financials) should be submitted.
v. At least One Work order should be minimum value of Rs. 6.00 crores. Copy of the work order to be submitted, should not be more than 3 Years old.
vi. Copy of Incorporation certificate of the company should be submitted.
vii. Manufacturers Authorization Form (MAF)/Certificate from OEM details such as name, designation, address, e-mail Id and Phone No. required to be furnished along with the bid for back-to-back support*.
viii. The bidder should submit acceptance to GeM bid and ATC, if compliance is not submitted it will be presumed as non-acceptance of bidder to GeM bid conditions and ATC.
ix. The bidder should submit details of OEM Make and Model with compliance to technical specifications in Annexure-III of this document.

x. Complete Data Sheet of offered equipment and Models.
xi. Compliance for non-violation of IPR i.e. copyright, trademarks, patents and design should be submitted by bidder on latter head of the company.
xii. An online complaint management & reporting system should be available.

***CSCSPV reserves right to verify All MAF (OEM) during technical evaluation.**

Bidders should submit EMD; undertakings on judicial stamp papers (original documents) to the office on or before closing date of bid for verification at the time of technical qualification bid. Successful bidders meeting technical qualification criteria after verification of uploaded documents with original bidder should be allowed to consider for technical evaluation. Bidders are required to upload all documents supporting technical evaluation.

***b) Technical Evaluation:***

The technical evaluation will be done only for the proposals submitted by the Companies fulfilling all prequalification criteria as mentioned in Annexure I. The capability and eligibility of the Bidder shall be determined based on the information provided by the Bidder i.e. experience in the field, presence of the Bidder at multiple locations, manpower strength, etc. The bidder would be considered technical qualified based on observation of the technical committee on details of the components duly specified by bidder in Annexure III.

***c) Financial Evaluation:***

- The financial evaluation shall be based on the total cost charged on CSCSPV.
- The Financial bid shall consider all expenses, statutory liabilities, tax liabilities and all associated costs, whatsoever. For the avoidance of doubt, it is clarified that all taxes shall be deemed to be included in the Financial Bid. The total cost should be stated clearly inclusive of all applicable taxes. The Financial Bid shall be submitted in INR only.
- The rate once quoted by a vendor cannot be changed later on during the contract period.
- Conditional bids/offers will summarily be rejected. Also, the bids which do not conform to terms and conditions of the bid document are liable for rejection out rightly.
- Any bid with zero/NIL/N.A./Blank service charges will be rejected summarily and O/o CSCSPV will not be held responsible, whatsoever, for any clarification on rejection of bid.
- CSCSPV will not make any other payment other than specified in the bid.
- The total amount indicated in the Financial Bid shall be unconditional, unequivocal, final, and binding on the bidder. If any assumption or condition is indicated in the Financial Proposal, it shall be considered as non-responsive, and the proposal shall be rejected.
- The bidder has to comply in writing the assurance of supply of all the items specified in the bid.

**K. SPECIAL CONDITIONS OF CONTRACT:**

a) In the specification wherever support for a feature, accessories has been asked for, it will mean that the feature, accessories should be available without CSC SPV requiring any other hardware/ software/ licenses. Thus, all hardware/ software/ licenses required for enabling the support/feature/accessories shall be included in the offer.

b) The equipment offered shall have complete data sheets and detailed descriptions on OEM web sites. Bidders are required to submit duly filled and signed technical compliance of the equipment's/systems offered in Annexure-III, failing which the bids may be rejected.

c) The bidder shall submit the detailed Bill of Material (BOM) of the equipment offered duly verified and certified by the respective OEM.

d) GSTIN ID of vendor should be provided from where goods will be supplied.

e) The Bidder will submit his bid after examining the bid documents, the scope of work, specifications, clauses, additional terms of contract agreement, special terms & conditions, bill of quantities, etc.

f) If a Bidder whose bid is accepted and fails to supply and install the equipment on specified locations as per the date of issue of the award letter, the earnest money deposited will be forfeited and no payment will be given for the work done by the vendor.

g) O/o CSCSPV does not bind itself to accept the lowest or any bid and reserves the right to reject any or all bid without assigning any reason.

h) O/o The CSCSPV will not pay any expense, whatsoever incurred by the Bidder for the preparation and submission of bid.

i) This notice inviting bid will form part of the contract agreement to be executed by the successful Bidder with "O/o CSCSPV, New Delhi".

j) Correspondence, if any, on the bidder shall be addressed to CSC e-Governance Services India Limited, 238, Okhla Industrial Estate, Okhla Phase-III, New Delhi, 110020, and any communication addressed to any other person shall not in any manner to be binding upon the O/o CSCSPV.

k) Even though the applicants may meet the above criteria, they are subject to be disqualified if they have:

   i. Made misleading or false representation in the form, statement, documents and attachments submitted, or

   ii. Record of poor performance such as abandoning the work, not properly completing the contract, inordinate delays in completion, litigation history, or financial failures, etc., or

   iii. Found to have been blacklisted in any work assigned by the department earlier which was not completed within the prescribed period and rest of the work being completed by the department from another vendor, or

   iv. Conditional bidder or Telegraphic bidder or Bidder containing remarks uncalled for, or Bidder not submitted on prescribed Performa or Bidder submitted late shall be rejected.

n) The Bidder shall stamp and sign (with name of signatory) at the bottom right-hand corner of every page of the bidder documents in token of acceptance of bidder conditions and for the purpose of identification.

o) No advance payment will be made to the Bidder.

p) CSC SPV reserves the right to forfeit the earnest money deposit (EMD) if the Bidder fails to commence signed contract the work within the stipulated time.

q) The Bidder shall ensure that all the staff deployed by the agency at the site shall be suitably qualified with adequate experience in carrying out the installation work covered in the scope of work.

r) Security staff shall be at liberty to exercise check on any of the workers, supervisors while entering and while leaving from the premises during installation and warranty period.

s) The condition of yearly average annual turnover and prior experience may be relaxed for Startups as per rule 173 (i) of General Financial Rules (GFRs) - 2017, subject to meeting the other criteria as mentioned in herein.

t) As soon as any defect is noticed in any of the equipment / accessories, the same will be brought to the knowledge of the Head of the office, CSCSPV offices or his authorized representative for each location or address mentioned.

**Testing and Inspection:**

u) CSC SPV or its representative shall have the right to inspect or to test the Equipment to confirm their conformity to the ordered specifications. The supplier shall provide all reasonable facilities and assistance to the inspecting authority at no charge to CSC. In case any inspected or tested equipment fail to conform to the specifications, CSC may reject them, and supplier shall replace the rejected equipment with the equipment in conformity with the specification required free of cost to CSC.

Commented [A1]: CSC SPV

**Force Majeure:**

v) CSC SPV may grant an extension of time limit set for the completion of the work / repair in case the timely completion of the work is delayed by force majeure beyond the contractor's control, subject to what is stated in the following sub paragraphs and to the procedures detailed there-in being followed. Force Majeure is defined as an event of effect that cannot reasonably be anticipated such as acts of God (like earthquakes, flood, storms etc), acts of states, the direct and indirect consequences of wars (declared or un-declared), hostilities, national emergencies, civil commotion, and strikes (only those which exceed a duration of ten continuous days) at successful Bidder's factory.

**n. Scope of Work:**

1. Supply of Data Center equipment {Servers & Storage, Network Equipment, Firewall, all required Hardware & Software including licenses} with 5 Years warranty & perpetual license, if any, at addresses mentioned as above.
2. After the supply of equipment as mentioned in the Annexure III, the bidder and OEM must execute design and planning of installation, Migration from existing equipment & commissioning at the designated location(s). No extra cost shall be paid for this reason by the buyer.
3. Delivery & Installation documents should be submitted by the successful bidder with duly signed & acceptance of CSC SPV officer designate.
4. The bidder/OEM shall offer on-site comprehensive warranty of Five (05) years from the date of successful commissioning of the required equipment at the designated location. The buyer is not liable to pay any extra charges on any account during the warranty period.
5. All the accessories required for the deployment of the equipment are in the scope of the bidder, no extra accessories, equipment, cable, connector etc. will be provided by CSC SPV. Bidder has to submit the acceptance on the Company Letter Head. All Clarification should be taken by bidder before any execution and participation.
6. OEM Warranty details should be submitted with the Installation Report {OEM Device Portal Details, Support SPOC Details, Device Support Category Details, License Details, Component details etc.)
7. Successfully transition of the offered devices and solution for any migration, with minimal disruption to network outages in the data center. Migration should be planned after CSC SPV Business Hours i.e. between 10PM to 5AM.

**Testing and Validation**

- Perform thorough testing of the configured equipment in the current infrastructure with CSC SPV Officials to ensure it meets performance and security requirements.
- Validate that all equipment, rules and policies are functioning as expected.

**Timeline to be share by the bidder**

Define the project timeline, including key milestones and deadlines.

- **Roles and Responsibilities**
- **Project Kickoff:** [Start Date]
- **Current State Assessment Completion:** [Date]
- **Solution Selection and Approval:** [Date]
- **Planning and Design:** [Date]
- **Implementation Start Date:** [Date]
- **Testing and Validation:** [Date]
- **Project Completion:** [End Date]
- **Acceptance Testing:** [Date]
- **Knowledge Transfer**
- **Support After the deployment**

# Annexure I

## Product Make & Model / Commercial Offer – Data Center Devices

| # | Item Specification as per Annexure III | Make and Model | Quantity (nos.) | Price Without Taxes | | | Taxes | Total Price including 5-year Warranty + Support |
|---|---|---|---|---|---|---|---|---|
| | | | | Unit price including 1 Year warranty and support | Unit Price including 3 Years warranty and support | Unit Price including 5 Years warranty and support | | |
| 1 | Storage Nodes (Server Type-1) | | **3** | | | | | |
| 2 | Monitor and Mgmt. Node (Server Type -2) | | **3** | | | | | |
| 3 | Compute Node (Server Type-3) | | **3** | | | | | |
| 4 | Data Center Network Switches | | **4** | | | | | |
| 5 | Office Network Firewall | | **2** | | | | | |
| 6 | General Purpose Hardware Security Module (HSM) | | **2** | | | | | |
| 7 | Financial Hardware Security Module {F.HSM} | | **2** | | | | | |
| 8 | Zimbra Enterprise e-Mail Solution (Existing Upgrade) | | **1** | | **NR** | **NR** | | **With 2 Y Support** |
| **Total** | | | | | | | | |

*** Offered Commercial is mandatory to be provided in the above format.**

*** Taxes should be mentioned in the specific column titled taxes.**

**NR – Note Required**

**Note: -**

1. Please refer the specifications in Annexure-III. Rates quoted should be inclusive of all required accessories, Cables, Connectors, Modules, Licenses etc. CIP to the destination.
2. Compliance to the specifications as given in Annexure-III should be duly filled and signed by the bidder, failing which it may result in rejection of the bid.
3. Equipment will not only be selected on the basis of commercial, the equipment & OEM Experience and Class will also be considered at the time of device finalization.
4. Equipment and Equipment Quantity will be finalized by Buyer at the time of final Work Order / LOI.
5. The OEM should provide 24x7x365 days (including Sunday, holiday etc.) technical support. The OEM should provide the login credentials with highest level permission to raise the technical issues, search knowledge base, download the patches & upgrade, documents and manage the device on OEM website.
6. The offered devices model should not be End of Life/End of Support in near Future or within 1-5 Year from the data of Work Order.

## Annexure II

**Performa for Manufacturer Authorization form (MAF)**

The O/o CSCSPV, Dated: .....

.....

.....

.....

Subject: Manufacturer Authorisation form (MAF) to M/s for .....

Ref: GeM Bid No..... dated.....

Dear Sir,

We, M/s....., are established and reputed manufacturer and service provider of ..... (Product details), having our registered office at ..... .....

We hereby authorise M/s..... (bidder name), Office.

..... to participate in the bid and subsequently upon award of the bid to execute the supply and Installation & Commissioning of our range of products against your above said bid.

We further extend our warranty for five (05) years for our range of products offered by M/s.....

..... against the above-said bid.

Thanking you,

Best regards,

Authorized Signatory

# Annexure III

**Specifications for Data Center equipment**

* Minimum Technical Specification details are mentioned below.

** Specification & Compliance sheet to be duly signed &submit by the bidder with eligibility.

*** Equipment Quantity may vary at the time of final Work Order allotment to bidder

**** The required solution must not be End of Life or End of Support for at least 5 years from the due date of submission of bid by the bidder.

## 1. Storage Nodes (Server Type-1)

| | Server Specification | |
|---|---|---|
| **S.NO.** | **Minimum Technical Specification** | **Compliance (Yes/No)** |
| | **Required Features** | |
| 1 | The proposed Rack Server should be 2RU form factor with 24 SFF slots | |
| 2 | Each Server should have minimum 2 X Intel/AMD Processors, each processor should have 32 Cores, 64 Threads with base clock speed 2.4GHz or above | |
| 3 | Each Server have RAM populated using DDR5 Module. Each node should have total 512 GB of RAM. | |
| 4 | Each Server should be supplied with 2 X RAID Storage Controller with 4GB Cache. It should support RAID Levels 0, 1, 5, 6, 10. Drive support SATA, SAS, NVMe Ports x 8 host / x16 internal. Also the server should be supplied with Battery Backup unit with cable kit | |
| 5 | Each Server should be supplied with 20 x 15 TB NVMe RI SSD | |
| 6 | Each Server should be supplied with 2 x 1.9 TB NVMe RI SSD | |
| 7 | Each Server should have 4 x dual port 10/25G SFP+ Network adaptor, with 16* x 10/25G SFP+ SR modules Populated in all Ports | |
| 8 | The proposed server should support features such as Intelligent Platform Management Interface Version 2, secure boot, UEFI shell, PXE boot, SNMP v2 & v3, HTML 5 GUI, CLI, SMTP, XML API/redfish API, Virtual console, energy star, TPM 2.0, PCIe 3.0 compliance | |
| 9 | The proposed Server Should have extra empty storage Slots for future expansion. | |

| | | |
|---|---|---|
| 10 | The proposed server should have redundant hot swappable high efficiency power supplies, redundant fan modules, Trusted Platform Module 2.0, 2 x USB 3.0 ports, 1 x VGA/Display/KVM port, one out of band management port, 2* x 10G RJ 45 ports, 2 x PCIe 3.0 slots | |
| 11 | The proposed Server should support hypervisor such as ESXi, Hyper-V, KVM, RHEV, AHV. | |
| 12 | The proposed Server should be industry standard x86 servers | |
| 13 | The Server should support monitoring via SNMPv3 and email alerting via SMTP | |
| 14 | The Server should be a tested and validated to run MS SQL, PostgreSQL, MongoDB, OpenStack, Virtual machines, Windows Server OS, RHEL OS & Containers. | |
| 15 | The proposed server should be supplied with the licenses for remote console configuration & monitoring of the server through GUI | |
| 16 | The proposed Server should be supplied with 5 Years warranty & 5 years 24x7x365 OEM support | |
| 17 | The proposed should integrate with AD/LDAP for Authentication | |
| 18 | The proposed server OEM should be minimum 10-year-old organization and should have the corporate/support offices in India | |
| 19 | The bidder should submit bid specific OEM MAF certificate | |
| 20 | All the required Cables to connect the all interface in server should be supplied without any additional cost | |
| 21 | The proposed Server should be supplied with 5 Years warranty with maximum 6 hrs. onsite part replacement service & 5 years 24x7x365 OEM support | |
| 22 | Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD | |
| 23 | Real-time out-of-band hardware performance monitoring & alerting, Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health, Out-of-band hardware & firmware inventory, Automated hardware configuration and Operating System deployment to multiple servers, Virtual IO management / stateless computing | |
| 24 | Automated deployment of Server Config profiles. Import/Export of the server configuration profile need to be showcased on the Management software | |

| | | |
|---|---|---|
| 25 | Telemetry streaming - Continuous stream metrics from a server. Information about the health status of the server & HDD need to be showcased.<br>Note: Appropriate License for the management software needs to be factored. | |
| 26 | Seamless firmware updates. Should be able to create firmware and configuration baselines for compliance monitoring and enable automated updates on schedule | |
| 27 | Secure firmware updates - Cryptographic signed firmware updates, required to be showcased | |
| 28 | In case of any security breach the server should get locked, when the threat/breach is removed the server should start from the same state of firmware when it got locked. | |

**2. Management, Controller, Monitor Node (Server Type-2)**

| | **Server Specification** | |
|---|---|---|
| **S.NO.** | **Minimum Technical Specification** | **Compliance (Yes/No)** |
| | **Required Features** | |
| 1 | The proposed Rack Server should be 2RU form factor with 24 SFF slots | |
| 2 | Each Server should have minimum 2 X Intel/AMD Processors, each processor should have 24 Cores, 48 Threads with base clock speed 2.4GHz or above | |
| 3 | Each Server have RAM populated using DDR5 Module. Each node should have total 256 GB of RAM. | |
| 4 | Each Server should be supplied with 2 X RAID Storage Controller with 4GB Cache. It should support RAID Levels 0, 1, 5, 6, 10 . Drive support SATA , SAS, NVMe. Ports x 8 host / x16 internal. Also the server should be supplied with Battery Backup unit with cable kit | |
| 5 | Each Server should be supplied with 4 x 1.9 TB NVMe RI SSD | |
| 6 | Each Server should have 4 x dual port 10/25G SFP+ Network adaptor , with 16 x 10/25G SFP+ SR modules | |
| 7 | The proposed server should support features such as Intelligent Platform Management Interface Version 2, secure boot, UEFI shell, PXE boot, SNMP v2 & v3, HTML 5 GUI, CLI, SMTP, XML API/redfish API, Virtual console, energy star, TPM 2.0, PCIe 3.0 compliance | |

| | | |
|---|---|---|
| 8 | The proposed server should have redundant hot swappable high efficiency power supplies, redundant fan modules, Trusted Platform Module 2.0, 2 x USB 3.0 ports, One VGA/Display/KVM port, one out of band management port, 2 x 10G RJ 45 ports, 2 x PCIe 3.0 slots | |
| 9 | The proposed Server should support hypervisor such as ESXi, HyperV, KVM, RHEV, AHV | |
| 10 | The proposed Server should be industry standard x86 servers. | |
| 11 | The Server should support monitoring via SNMPv3 and email alerting via SMTP. | |
| 12 | The Server should be a tested and validated to run MS SQL, PostgreSQL, MongoDB, OpenStack, Virtual machines, Windows Server OS, RHEL OS & Containers. | |
| 13 | The proposed server should be supplied with the licenses for centralized configuration & monitoring of the server through GUI | |
| 14 | The proposed should integrate with AD/LDAP for Authentication | |
| 15 | The proposed Server should be supplied with 5 Years warranty with 6 hrs onsite part replacement service & 5 years 24x7x365 OEM support | |
| 16 | The proposed server OEM should be minimum 10-year-old organization and should have the corporate/support offices in India | |
| 17 | Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD | |
| 18 | Real-time out-of-band hardware performance monitoring & alerting<br>Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health<br>Out-of-band hardware & firmware inventory<br>Automated hardware configuration and Operating System deployment to multiple servers<br>Virtual IO management / stateless computing | |
| 19 | Shall provide Chassis Intrusion detection even when no power is available. | |
| 20 | Automated deployment of Server Config profiles. Import/Export of the server configuration profile need to be showcased on the Management software | |

| | | |
|---|---|---|
| 21 | Automated renewal and installation for Management software SSL Certificate need to be showcased | |
| 222 | Alarm for Chassis intrusion protection - Alarm even when both PSUs are not plugged in | |
| 23 | Secure firmware updates - Cryptographic signed firmware updates by Dell. Need to be showcased by flashing the network card firmware or HDD firmware upon downloading directly from the vendor's website | |
| 24 | Telemetry streaming - Continuous stream metrics from a server. Information about the health status of the server & HDD need to be showcased. Note : Appropriate Licence for the management software needs to be factored | |
| 25 | System Lockdown - It should prevent unintended changes after a system has been initially configured. Lockdown mode applicable to both configuration and firmware updates needs to be shown | |
| 26 | Seamless firmware updates. Should be able to create firmware and configuration baselines for compliance monitoring and enable automated updates on schedule | |
| 27 | In case of any security breach the server should get locked, when the threat/breach is removed the server should start from the same state of firmware when it got locked. | |

### 3. Compute Nodes (Server Type-3)

| | **Server Specification** | |
|---|---|---|
| **S.NO.** | **Minimum Technical Specification** | **Compliance (Yes/No)** |
| | **Required Features** | |
| 1 | The proposed Rack Server should be 2RU form factor with 24 SFF slots | |
| 2 | Each Server should have minimum 2 X Intel/AMD Processors, each processor should have 32 Cores, 64 Threads with base clock speed 2.4GHz or above | |
| 3 | Each Server have RAM populated using DDR5 Module. Each node should have total 1024 GB of RAM. | |
| 4 | Each Server should be supplied with 2 X RAID Storage Controller with 4GB Cache. It should support RAID Levels 0, 1, 5, 6, 10. Drive support SATA, SAS, NVMe Ports x 8 host / x16 internal. Also the server should be supplied with Battery Backup unit with cable kit | |

| | | |
|---|---|---|
| 5 | All Ports should be populated with required modules. | |
| 6 | Each Server should be supplied with 2 x 1.9 TB NVMe RI SSD | |
| 7 | Each Server should have 4 x dual port 10/25G SFP+ Network adaptor, with 16 x 10/25G SFP+ SR modules Populated in all Ports | |
| 8 | The proposed server should support features such as Intelligent Platform Management Interface Version 2, secure boot, UEFI shell, PXE boot, SNMP v2 & v3, HTML 5 GUI, CLI, SMTP, XML API/redfish API, Virtual console, energy star, TPM 2.0, PCIe 3.0 compliance | |
| 9 | The proposed Server Should have extra empty storage Slots for future expansion. | |
| 10 | The proposed server should have redundant hot swappable high efficiency power supplies, redundant fan modules, Trusted Platform Module 2.0, 2 x USB 3.0 ports, One VGA/Display/KVM port, one out of band management port, 2 x 10G RJ 45 ports, 2 x PCIe 3.0 slots | |
| 11 | The proposed Server should support hypervisor such as ESXi, Hyper-V, KVM, RHEV, AHV. | |
| 12 | The proposed Server should be industry standard x86 servers | |
| 13 | The Server should support monitoring via SNMPv3 and email alerting via SMTP | |
| 14 | The Server should be a tested and validated to run MS SQL, PostgreSQL, MongoDB, OpenStack, Virtual machines, Windows Server OS, RHEL OS & Containers. | |
| 15 | The proposed server should be supplied with the licenses for remote console configuration & monitoring of the server through GUI | |
| 16 | The proposed Server should be supplied with 5 Years warranty & 5 years 24x7x365 OEM support | |
| 17 | The proposed should integrate with AD/LDAP for Authentication | |
| 18 | The proposed server OEM should be minimum 10-year-old organization and should have the corporate/support offices in India | |
| 19 | The bidder should submit bid specific OEM MAF certificate | |
| 20 | All the required Cables to connect the all interface in server should be supplied without any additional cost | |
| 21 | Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD | |

| | | |
|---|---|---|
| 22 | Real-time out-of-band hardware performance monitoring & alerting<br>Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health<br>Out-of-band hardware & firmware inventory<br>Automated hardware configuration and Operating System deployment to multiple servers<br>Virtual IO management / stateless computing | |
| 23 | Shall provide Chassis Intrusion detection even when no power is available. | |
| 24 | Automated deployment of Server Config profiles. Import/Export of the server configuration profile need to be showcased on the Management software | |
| 25 | Automated renewal and installation for Management software SSL Certificate need to be showcased | |
| 26 | Alarm for Chassis intrusion protection - Alarm even when both PSUs are not plugged in | |
| 27 | Secure firmware updates - Cryptographic signed firmware updates by Dell. Need to be showcased by flashing the network card firmware or HDD firmware upon downloading directly from the vendor's website | |
| 28 | Telemetry streaming - Continuous stream metrics from a server. Information about the health status of the server & HDD need to be showcased. Note : Appropriate Licence for the management software needs to be factored | |
| 29 | System Lockdown - It should prevent unintended changes after a system has been initially configured. Lockdown mode applicable to both configuration and firmware updates needs to be shown | |
| 30 | Seamless firmware updates. Should be able to create firmware and configuration baselines for compliance monitoring and enable automated updates on schedule | |
| 31 | In case of any security breach the server should get locked, when the threat/breach is removed the server should start from the same state of firmware when it got locked. | |

**4. Data Center Network Switch**

| | Network Switches | |
|---|---|---|
| **S.NO.** | **Minimum Technical Specification** | **Compliance (Yes/No)** |
| 1 | **Required Features -** Hardware and Form factor Specifications | |
| | Switch shall be 1 RU and rack mountable in standard 19" rack. | |
| | Switch shall be based on Multicore CPU to run multiple process simultaneously | |
| | Modular architecture or fixed form architecture, with necessary redundancy for Fan and Power supply | |
| | Switch should have Redundant Power Supply and Fans | |
| | The Switch should support non-blocking architecture, all proposed line cards/transceivers must provide wire speed line rate performance | |
| | Switch shall have 16 GB RAM and 16 GB Flash | |
| | Switch should have 48 x 1/10/25G SFP+ ports | |
| | Switch should have 4 x 40/100G QSFP ports | |
| | Switch shall support Virtualization Technology to represent 2 different switches, appear as one to the downlink/uplink switches and should be able to support L2/L3 redundancy among themselves with minimal disruption | |
| | Switching system shall have minimum 3 Tbps of switching capacity | |
| | Switching System should support minimum 1 Tbps of forwarding rate. | |
| | Shall support up to 512 VLANs. | |
| | Switch should support 30 MB packet buffer | |
| | Switch should support 80K MAC addresses | |
| | Switch should support minimum 60K IPv4/ IPv6 Routes | |
| | Switch should support minimum 30K multicast routes | |
| | Switch software should provide option to program the switch hardware to allocate required resources appropriately. | |

| | | |
|---|---|---|
| | Shall support GARP VLAN Registration Protocol or equivalent feature to allow automatic learning and dynamic assignment of VLANs. | |
| | Should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.1ae (256-bit and 128-bit AES), 802.3x, 802.1p, 802.1Q, 1588v2 | |
| | Should support MACSEC-256 encryption algorithm on hardware on all ports (Uplink and Downlink) | |
| | Must support BGP, MPLS, IS-IS, VRF, VXLAN, NAT, OSPF, Policy-Based Routing (PBR), PIM SM, VRRP/equivalent features from Day 1 | |
| | Shall have 802.1p class of service, marking, classification, policing and shaping. Should support strict priority queuing. | |
| | Switch should support management features like SSHv2, SNMPv2c, SNMPv3, IGMP, Link Layer Discovery Protocol (LLDP). | |
| | Switch should support port security, DHCP snooping, Spanning tree root guard, First Hop Security. | |
| | Switch should support IPv4 & IPv6 from day1. | |
| | Should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment. | |
| | Access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network. | |
| | RADIUS/TACACS for switch security access administration | |
| | Switch should support eight egress queues per port for different types of traffic. | |
| | Switch shall support Virtual Stacking or equivalent features allows links that are physically connected to two different switch to appear as a single port channel | |
| | During system boots, the system's software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic | |
| | Switch should support comprehensive programmability features like Model-Driven Programmability, NETCONF/REST API interface | |

| | | |
|---|---|---|
| | Operating temperature of 0°C to 40°C. | |
| | The device should be IPv6 certified from day one | |
| | Switch shall conform to UL 60950, IEC 60950, CSA 60950, EN 60950 Standards | |
| | Switch / Switch Series/ Switch's Operating System should be tested for EAL 2/NDPP/NIAP/NDcPP or above under Common Criteria Certification. | |

**5. Office Firewall**

| | **Firewall & Security Device** | |
|---|---|---|
| **S.NO.** | **Minimum Technical Specification** | **Compliance (Yes/No)** |
| 1 | **Required Features** | |
| | The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems. Firewall must be supplied with gateway Anti-malware, IPS/IDS, Application control , Web filtering with 24*7*365 OEM TAC support for **5 years**. | |
| | The Proposed Firewall Vendor should be SOC2 compliant which covers security, availability, processing integrity, confidentiality, and/or privacy controls. OEM must have ISO:27001 certification. | |
| | The Firewall should support integration of on Premises sandbox of same OEM in future | |
| | Software upgrades, updates shall be included as part of the warranty | |
| | The Firewall & IPSEC VPN module shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification. | |
| | Operating temperature of 0°C to 40°C | |
| | All mentioned features (above & below) should be available from Day One. Any license required to be factored from Day One with 5 Years License and support | |
| | The offer solution should be in OEM warranty RMA and technical support for 5 Years from the date of issuance of | |

| | | |
|---|---|---|
| | completion certificate with onsite service inclusive of labor and parts for complete solution.<br>The required support shall include minimum following.<br>• Next Business Day RMA support<br>• Free Software Upgrade, Documentation along with support for upgradation from OEM TAC<br>• 24X7 Telephone diagnosis support from OEM TAC | |
| 2 | **Performance** | |
| | Should be able to run all required features and new firmware updates for the next five years without experiencing any performance deterioration with enough CPU cores and memory from day one. | |
| | Firewall throughput should be minimum 4.2+ Gbps or higher from day one on single appliance. | |
| | Firewall should have minimum 2.5 Gbps or higher of IPSEC VPN throughput or higher from Day One on single appliance. | |
| | Firewall should support site-to-site & client to site VPN Tunnels. | |
| | Firewall should have 50,000+ new sessions per second or higher from day one | |
| | Firewall should have 1M concurrent sessions from day one | |
| | Proposed Firewall must have SSL Inspection from day one. Inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2.Offers rich visibility into TLS traffic, such as amount of encrypted traffic, TLS/SSL versions, cipher suites, and more, without decrypting. | |
| | The solution should have minimum 2.3 Gbps of threat protection (FW + IPS + Application control + Antivirus ) throughput of mix/production traffic or higher from day one. | |
| | Proposed appliance must have minimum 256 GB+ SSD storage capacity and Appliance must have dual redundant power supply from day one. | |
| | Should support the ability to auto backup of the previous configuration automatically. | |
| | QoS : Solution should support the ability to create QoS Policy:<br>• by destination address<br>• by user/user group as defined by AD<br>• by application ( such as Skype, Bit torrent, YouTube)<br>• by static or dynamic application groups (such as instant | |

| | | |
|---|---|---|
| | • Messaging or P2P groups) and-by post | |
| | The proposed firewall shall define Qos traffic classes and shall support real-time prioritization of traffic | |
| 3 | **Functionality:** | |
| | The NGFW solution should support NAT64, NAT66, DNSv6 & DHCPv6 along with Virtual Domain / systems | |
| | The NGFW should support WAN links load balancing and fail-over for at least 4 links | |
| | NGFW must have option to rate web resource based on their DNS rating, | |
| | The proposed system should have integrated Traffic Shaping functionality. | |
| | The proposed system should support : IPSEC VPN, PPTP VPN. | |
| | The device shall utilize inbuilt hardware VPN acceleration: IPSEC (DES, 3DES, AES) encryption and decryption, SSL encryption/decryption, | |
| | The system shall support the following IPSEC VPN capabilities: VPN supports, IPSec, ESP security, Supports NAT traversal, Supports Hub and Spoke architecture, Supports Redundant gateway architecture. | |
| | The system shall support IPSEC site-to-site VPN and remote user VPN. | |
| | The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN. | |
| | Microsoft AD, LDAP, RADIUS, NAT, Firewall, VPN (Ipsec), VPN (SSL), Identity Awareness, Content Awareness, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot, DNS Security, CASB Database, DLP, prevention of known and Zero day Attack. | |
| 4 | **Intrusion Prevention System** | |
| | The solution should have minimum 2.3 Gbps of threat protection (FW + IPS + Application control + Antivirus ) throughput of mix/production traffic or higher from day one. | |
| | IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available | |

| | | |
|---|---|---|
| | In event if IPS should cease to function, it will fail open by default and is configurable. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved | |
| | IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups. | |
| | IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident | |
| | Signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low) | |
| 4 | **Interface Requirement** | |
| | Firewall appliance should have minimum 10 x 1GE , 4 x 1G/10G SFP/SFP+ from Day One. All the ports should be fully populated with required modules to meet the mentioned speed from day one. | |
| 5 | **Antivirus Features** | |
| | The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services: HTTP, HTTPS, SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS, FTP, FTPS | |
| | The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database. | |
| | The proposed solution should be able to perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero- day and targeted attacks. | |
| | The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy. | |
| | The NGFW must have option to rate web resource based on their DNS rating | |

| | | |
|---|---|---|
| | NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time before passing it to user. | |
| | NGFW should allow administrator to prevent sensitive data from leaving the network. Administrator should be able to define sensitive data patterns, and data matching these patterns that should be blocked and/or logged when passing through the unit. | |
| | NGFW must detect, protect and log sensitive data travelling through protocols - HTTP, FTP, SMTP, IMAP, POP3, NNTP, MAPI, CIFS, SFTP, SCP | |
| 6 | **Web Content Filtering:** | |
| | The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules. | |
| | The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic. | |
| | The proposed system shall provide web content filtering features:<br>a) Inbuilt Captive portal for users to allow access to internet.<br>b) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies.<br>c) Shall include Web URL block<br>d) Shall include score based web keyword block<br>e) Shall include Web Exempt List | |
| | The proposed system shall be able to queries a real time database of over 200 million + rated websites categorized into unique content categories. | |
| 7 | **High Availability:** | |
| | Firewall should support Active/Standby and Active/Active failover and should not be based on stacking units in clustering. | |
| | Firewall should support ether channel or equivalent functionality for the failover control and providing additional level of redundancy. | |
| | Firewall should support redundant interfaces to provide interface level redundancy before device failover. | |
| | High Availability Encryption should be supported | |
| | Firewall should support 802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment. | |

| | | |
|---|---|---|
| | Firewall should have redundant hot swappable power supply. | |
| 7 | **Application Control** | |
| | The proposed system shall have the ability to detect, log and take action against network traffic based on minimum 3K or higher application signatures | |
| | The application signatures shall be automatically updated | |
| | The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions | |
| | Solution should have capabilities to limit number of parameters in URL, number of cookies in request, number of headers lines in request, total URL and Body parameters in length to block advanced HTTP layer attacks. | |
| 5 | **Advance Threat Protection** | |
| | The Firewall solution should have detection and prevention capabilities for C&C communications and data exfiltration. Firewall should Identify and control network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create firewall rule lists to block the connection. | |
| | NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time before passing it to user. | |

### 6. General Purpose Network Hardware Security Module

| | **Firewall & Security Device** | |
|---|---|---|
| **S.NO.** | **Minimum Technical Specification** | **Compliance (Yes/No)** |
| 1 | **General Specifications** | |
| | The Purposed HSM should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems. HSM must be supplied with 24*7*365 OEM TAC support for **5 years.** | |

| | | |
|---|---|---|
| | The Hardware security module should be a network based general purpose hardware security module. Must Support Encryption, Digital Signing, Key Generation and Protection | |
| | Support for minimum 1000 Transaction (Signing) per Second @ RSA 2048 bits. | |
| | The HSM solution should ensure high availability, Failover with standby appliance at DC & DR via the HSM libraries and should not depend on any external load balancer | |
| | There should not be any limit on no. of Keys to be protected by HSM in accordance with FIPS 140-2 and CCA guidelines. Ability to generate and store the RSA keys (2048 and 4096) on board on demand and shall be secured inside HSM in accordance with FIPS 140-2 LEVEL 3 recommendations or equivalent. | |
| | There should not be any Limit on number of virtual partitions that can be created in HSM and number of keys that can be managed per partition. Each partition must support at least 2 Factor Authentication. | |
| | The proposed HSM Should have minimum 5 partitions along with supporting client licenses if required and each partition should be protected with unique set of user id and password and 2 FA to grant access as per CCA guidelines. Mention the existing partition with proposed HSM. | |
| | The proposed HSM should be capable of expanding Max 20 partitions on same HSM as business requirement may grows in future. | |
| | The required solution must not be End of Life or End of Support for at least 5 years from the due date of submission of bid by the bidder. | |
| | Support: OEM 24*7 support for HSM should be available. | |
| | The solution and all the components thereof must have provision for dual hot-swappable power supply. | |
| | Support of Functionality Modules to run custom code within the secure boundary of the FIPS 140-2 Level 3 or FIPS 140-2 Level 3 certified HSM. | |
| | There should be no root or super-user access to HSM appliance possible in any way. No access to bash, ksh or any default terminal shells should be possible. | |
| | HSM appliance should be FIPS 140-2 level 3 certified or equivalent. | |
| | Supported OS - Windows, RHEL, SUSE, Oracle Ent., Linux, Solaris (SPARC), IBM AIX, HP-UX and major cloud service | |

| | | |
|---|---|---|
| | providers running as virtual machines or in containers, Open Source system etc. | |
| | All Keys including private keys must be stored and protected within FIPS 140-2 Level 3 validated storage of the HSM. | |
| | Ability to monitor and detect Voltage and Temperature should be available. | |
| | HSM should have the ability to enable / disable policies by HSM commands which will be applicable for Application Users. This feature should not need any Application User login or credentials. | |
| | Synchronization of keys between HSMs on real-time basis | |
| | Support for migration of existing keys from current HSM through high availability | |
| | The proposed HSM should ensure seamless migration of existing keys with upmost security without taking the keys out in plain format as well no separate downtime requirement, if any. | |
| | The proposed HSM should also ensure that the existing application continue to work without any change in the code. Must have an ability to provide a secure environment for running sensitive applications within HSM boundaries | |
| | Should Support remote administration for maintaining partitions and adding or removing partitions as business required without the need for accessing HSM physically. | |
| | Signed and tamper-evident event based audit logs and standard mechanisms for viewing logs should be available. | |
| | HSM should be minimum 1U, Rack mountable | |
| | HSM Should have Minimum Two Gigabit Ethernet Ports | |
| 2 | **Cryptographic Features Requirement** | |
| | Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA, and more | |
| | Symmetric: AES, AES-GCM, DES, Triple DES, ARIA, SEED, RC2, RC4, RC5, CAST, Tiger HMAC and more | |
| | Hash/Message Digest/HMAC: SHA-1, SHA-2, SHA-3, MD5 and more | |
| | Full Suite B implementation with fully licensed ECC, including Brainpool and custom curves | |
| | Support APIs - PKCS#11, Java (JCA/JCE), Microsoft CAPI, nCore, Web Services Crypto API and CNG, OpenSSL | |

| | | |
|---|---|---|
| 3 | **Certification Requirement** | |
| | FIPS 140-2 Level 3 Validated | |
| | FIPS 140-3 Level 3 Validated (Preferred, in case all compliance validated under this certificate, as per RBI and other governance authorities) | |
| | BIS (India) for proposed model, BSI AIS 20/31 Compliant | |
| | Safety and Environmental standards - UL, CE, FCC, RCM, Canada ICES RoHS2, WEEE | |
| | IPV6 certified. | |
| | Performance: Flexible Scaling for RSA and ECC Signing, must support the range between 150 TPS to 10000+ TPS RSA Operations and Lower Latency and ECC upto 20000 TPS | |
| | Must support multiple and multi-level administration with Two factor authentication using smart cards on the same HSM device. | |
| | The HSM appliance and crypto card should be from the same OEM only and not as a bundled or assembled device. | |
| | The HSM should provide minimum 20 RSA 2048 key generations per second. | |

**7. Financial Hardware Security Module**

| | **Financial Hardware Security Module** | |
|---|---|---|
| **S.NO.** | **Minimum Technical Specification** | **Compliance (Yes/No)** |
| 1 | **General - Required Features** | |
| | The Purposed Solution should be supply with 24*7*365 OEM support for **5 years.** {Online and Offline, on premises} | |
| | Must Support load balancing, failover and High availability within the same cluster of HSMs | |
| | **Speed**: Minimum 25 CPS/TPS (Calls per second / Transactions per second). Should be upgradable above 60CPS for future requirement without replacing the Hardware. Stress testing to ensure stability under maximum load. | |
| | Form Factor - 1U 19" rack mount, Voltage – 90 to 264 VAC, Temperature Range- -25 deg C to 70 deg C, | |
| | Multiple LMK options – Minimum 3 Partitions with client licenses are required and support max up to 10 partitions Per HSM. | |

| | | |
|---|---|---|
| | HSM should have Dual hot swappable power supply and fans for redundancy. | |
| | Proposed Payment HSM should have Dual Gigabit Ethernet Interface, TCP/IP & UDP (1Gbps) – dual ports | |
| | The HSM proposed should be able to process upto 25 functions per second which include PIN translation and other payment functions from day 1 | |
| | The HSM proposed can be upgradable to Enhanced CPS (example 60 ~ 100) without any hardware changes. | |
| | The Proposed Payment HSM Support Multiple Partition for storing sensitive data for different Clients. | |
| | HSM should support RSA keys (up to 4096 bit),DES, 3DES KEY lengths 112 bit,168 bit and AES algorithm. | |
| | The proposed payment HSM should support multi-threading & multi-client so as maximum performance can be achieved. | |
| | The proposed payment HSM must be PCI-HSM 3.0 Certified or above. | |
| | The proposed payment HSM must be FIPS 140-2 Level 3 Certified. | |
| | The relevant security settings in the firmware should have PCI compliant values | |
| | HSM should offer seamless migration of keys from older generations of payShield, without any production downtime | |
| | OEM should have a support center in India and should have their own warehouse in India so that any Hardware support (RMA) can be provided easily & without any delay | |
| | The proposed HSM should support all the EFT standard cryptographic functions for debit and credit card management. | |
| | The proposed HSM should support all the EFT standard cryptographic functions for debit and credit card management. | |
| | Support Payment credential issuing – cards, mobile secure elements, wearables, connected devices and host card emulation (HCE) applications | |
| | Support both Magnetic stripe and EMV-based data preparation and personalization including mobile provisioning. | |
| | Should have GUI/CLI available with 2 factor authentication using USB Tokens/Smart Cards | |
| | Support SNMP and Utilization statistics - Health check diagnostic and error logs | |
| | The proposed HSM should support following Crypto Graphic Standard: AES, DES and Triple DES Algorithms - Provide PIN encryption, PIN Authorization and message authentication capabilities. | |

| | | |
|---|---|---|
| | The proposed payment HSM should support SHA-256 RSA 2048 Format or above. Capable to support DES and 3DES KEY lengths 112bit &168 bit and AES key lengths 128, 192 & 256 bits. | |
| **2** | **Security Features and Certification:** | |
| | Cryptographic module certified to FIPS: 140-2 Level 3 [certification is must] | |
| | Cryptographic module certified to FIPS: 140-3 Level 3 is preferred, in case all the compliance validated by the HS as describe by RBI [certification is must] | |
| | PCI HSM 3.0 Standard | |
| | The HSM appliance and crypto card should be from the same OEM only and not as a bundled or assembled device. | |
| | FIPS approved Random number generator | |
| | HSM remote management solution must have PCI HSM v3 Remote Access Platform (RAP) certification. | |
| | FIPS approved algorithms | |
| | Tamper resistance meeting requirements of PCI HSM 3.0 & FIPS 140-2 Level | |
| | Hash/message digest: SHA-1, SHA-2 (224,256,384,512 bit) | |
| | Sensitive data erased immediately in the event of any tamper attack | |
| | Payment HSM should have Dual Physical lock along with console cables | |
| | Two-factor authentication for the operator is must | |
| | HSM is implemented with secure PIN block format with controls to disable outputting PIN block in weaker format | |
| | Must support cryptographic offloading and acceleration | |
| | Access to the HSM should be controlled through Access Control Lists (ACLs) | |
| | Encryption Standard: 3DES to be used for data encryption. All sensitive transaction data to be encrypted with 3DES in compliance with security standards (e.g., PCI DSS).<br>Secure key exchange and management protocols to be included. | |
| | Symmetric algorithms: AES (key lengths upto 256 bit) , DES and Triple DES (key lengths upto 168 bit or higher) DUKPT,HMAC, MD5, SHA1, SH2, SHA3 AES key lengths 128, 192<br>& 256 bit | |
| | Variant-based master key for secure key hierarchy management. Documentation to include key derivation methodology and key rotation policies. | |
| | ISO 8583 Support: Fully enabled for transaction messaging. Support for parsing | |

| | | |
|---|---|---|
| | and constructing ISO 8583 messages. Field specifications and mapping details to be included in documentation. | |
| | BDK Generation:<br>BDK generation to be supported. Requirements for BDK implementation:<br>- Generation methodology and algorithm specifications.<br>- Integration with HSM for secure BDK storage and processing. | |
| | Supported Commands:<br>Support for M0/M1 and G0/G1 commands: Documentation to specify request/response formats, use cases, and error codes. | |
| | Secure Host communication using TLS or SSL | |
| 3 | **Financial Services Standards:** | |
| | ISO: 9564, 10118, 11568, 13491, 16609 | |
| | ANSI: X3.92, X9.8, X9.9, X9.17, X9.19, X9.24, X9.31, X9.52, X9.97 | |
| | ASC X9 TR-31, X9 TG-3/TR-39 | |
| | APACS 40 & 70 | |
| | | |
| 4 | **Cryptographic Algorithms** | |
| | DES and Triple-DES key lengths 112 & 168 bit | |
| | AES key lengths 128 bit, 192 bit & 256 bit | |
| | RSA (up to 4096 bits) | |
| | ECC as defined in FIPS 186-3 (P-256, P-384 & P-521) | |
| | HMAC, MD5, SHA-1, SHA-2, SHA-224, SHA-256, SHA-384 & SHA-512 | |

### 8. Zimbra Enterprise/Professional Edition Email Solution (Upgrade)

| | **Zimbra Enterprise/Professional Edition** | |
|---|---|---|
| **S.NO.** | **Minimum Technical Specification** | **Compliance (Yes/No)** |
| 1 | **General - Required Features** | |
| | The Purposed Solution should be supply with support for **2 years.** {Online and Offline, on Premises} | |
| | Existing single node Zimbra Mail server Community edition version upgrade (LTS Release) to Latest Professional / Enterprise LTS edition/Release. Security hardening and | |

| | | |
|---|---|---|
| | configuration best practice, HA, 2FA to be configured and support service to considered for **2 Years** | |
| | **Features**: User Interface, Search, Address Book, Web Clients, Calendar, Scheduling, Task activities, POP, SMTP, IMAP, Desktop Clients, Outlook Compatible, MAC Compatible, Backup, Archive, Smartphone application & Compatible with other digital devices etc. | |
| | Should be white Label, Multi-tenant Support, Should support setting up mail services on different domains in same instance | |
| | Support – Email & Phone Support (8 Hours X 5 Days) | |

**Note:**

**a)** Devices and components are required under 5 Year, 24x7 Warranty. Any Part replacement within 6 hrs. support, all the required licenses for the required features and functionalities should be supplied for 5 Years in the name of CSC e-Governance Services India Limited.

**b)** Single Bid for all required specified in the RFP.

**c)** Consortium Not Allowed.

**Annexure IV**
**DECLARATION BY THE Bidder (ON COMPANY LETTERHEAD)**

To

CSC e-Governance Services India Limited,
238, Okhla Phase-III, Okhla Industrial Estate,
New Delhi- 110020

Name of the Bidder -

Subject: Tender Reference Number CSCSPV/Data Center/2024-25/003 Supply and Installation of Data center equipment {Server & Storage, HSM, Network Equipment and Software} at different locations Pune (Maharashtra), Noida (Uttar Pradesh) and Okhla (New Delhi) under the administrative control of O/o CSC SPV, New Delhi.

Sir,

1. This is to certify that I/We before signing this bid have read and fully understood all the terms and conditions and instructions contained therein and undertake myself/ourselves abide by the said terms and conditions.

2. I/We hereby agree to pay the earnest money of amount as mentioned in the "Memorandum to this Form of Bidder" in favour of CSC e-Governance Services India Limited, payable at place as mentioned in the "Bid".

3. I/we are also enclosing herewith the Acceptance letter on the prescribed Performa as referred to in condition of Bid as Annexures.

4. If/We fail to commence the work within 15 days of the date of issue of Letter of Intent and/or I/we fail to sign the agreement as per contract and/or I/we fail to submit Performance Bank Guarantee as per contract, I/ we agree that CSCSPV, shall, without prejudice to any other right to remedy, beat liberty to cancel the Letter of Intent and to forfeit the said earnest money as specified above.

Dated the day of

SIGNATURE OF Bidder:

NAME (CAPITALLETTERS):

ADDRESS:

SEAL OF BIDDERER SIGNATURE OF WITNESS:

NAME (CAPITAL LETTERS) :

# Annexure V

## DECLARATION BY THE BIDDER (ON COMPANY LETTERHEAD)

To

CSC e-Governance Services India Limited,
238, Okhla Phase-III, Okhla Industrial Estate,
New Delhi- 110020

Name of the Bidder -

Subject: Tender Reference Number CSCSPV/Data Center/2024-25/003 Supply and Installation of Data center equipment {Server & Storage, HSM, Network Equipment and Software} at different locations Pune (Maharashtra), Noida (Uttar Pradesh) and Okhla (New Delhi) under the administrative control of O/o CSC SPV, New Delhi.

This is to certify that I/We will deliver the mentioned equipment in the Technical specification sheet at below mentioned locations and provide the 5 Years on-Site Warranty at these locations.

| Delivery Locations | Equipment Details |
|---|---|
| CSC e-Governance Services India Ltd, Plot Number 238, Okhla Phase 3 Rd, Okhla Phase III, Okhla Industrial Estate, New Delhi – 110020 | Will be confirmed at the time of WO/LOI |
| CSC e-Governance Services India Ltd, Plot#8, Sector – 106, Noida (UP) | Will be confirmed at the time of WO/LOI |
| CSC e-Governance Services India Ltd, WTC, Naroji Nagar, New Delhi | Will be confirmed at the time of WO/LOI |

{**Note:** Notify CSC SPV representatives in advance of any deliveries at the specified location.}

Dated the day of

SIGNATURE OF Bidder

NAME (CAPITALLETTERS):

ADDRESS:

SEAL OF BIDDERER SIGNATURE OF WITNESS

NAME (CAPITAL LETTERS) :