Open Tender Notification

for

Supply, Installation, Testing & Commissioning of the Firewall software.

Tender Enquiry No.: TPCODL/CCG/23-24/039

Due Date for Bid Submission: 25th October' 2023.

Centralized Contracts Group
(A TATA Power and Odisha Government Joint Venture)
TP Central Odisha Distribution Limited
1st Floor, Anuj Building, Plot No.29, Satya Nagar, Bhubaneswar – 751007

Tender Enquiry No - TPCODL/CCG/23-24/039

Tender Enquiry No.	Work Description	EMD (Rs.) *	Tender Fee (Rs.) incl. of GST**	Last Date and Time for payment of Tender Fee
TPCODL/CCG/23-24/039	Supply, Installation, Testing & Commissioning of the Firewall software.	18,00,000	5,000	10.10.2023

*** EMD is exempted for MSMEs registered in the State of Odisha.**

**** MSMEs registered in the State of Odisha shall pay tender fee of Rs. 1,000/- including GST.For details of MSME norms, pls refer "Annexure A" below.**

INFORMATION TO THE BIDDERS TO PARTICIPATE IN E-OPEN TENDER SYSTEM OF TPCODL

Steps for E-tender submission:

Bids are to be submitted only through an online e-procurement platform, ARIBA. Anyother form of bid submission will not be accepted. Online Link for submission of bid through ARIBA will be sent only after confirmation of payment of tender fee from bidder.

Step 1: The bidder can get primary information about the tender from the Newspaper advertisement / TPWODL/TPNODL/TPSODL website <www.tpcentralodisha.com> and can download the tender document from the above website.

Step 2: Non-Refundable Tender Participation Fee, as indicated in tender document, to be submitted before last date of tender fee payment, in the form of direct deposit/NEFT/RTGSin the following bank account.

Account Name: TP Central Odisha Distribution LimitedBank
Name: State Bank of India,
IDCO Towers, Bhubaneswar Bank
Account No.: 10835304915IFSC
Code: SBIN0007891

Step 3: Eligible and Interested bidder to send an email the documents duly signed and stamped letter on Bidder's letterhead, with following details, expressing their intent to bidagainst above tender:

Sl. No	Description	Bidder's Response
i)	Tender Enquiry No.	
ii)	Description of materials / Works Tendered	
iii)	Name and address of the bidding company	
iv)	Name of the authorized contact person	
v)	Contact No. authorized person	
vi)	E-mail Id of the where online ARIBA link to be mailed.	
vii)	Tender Fee details (Amount / NEFT-RTGS UTR No / Date),Ref step 2 above	
viii)	GST No. of bidder	
ix)	MSME Certificate, wherever applicable	
x)	Postal address of bidder for return of EMD BG	

The E-mail should be sent to saurabh.kumar@tpwesternodisha.com with copy to vipin.chauhan@tpnodl.com before "Last date and time for payment of Tender Participation Fee".

Step 4: On receipt of the document as mentioned in Step 3 above and after due verification of the same, ARIBA link for participation in the tender will be sent to bidder's mail address from ARIBA system.

Step 5: In this mail there will be an online link as **Click Here** to participate in the tender.

Step 6: Click **"Click Here"** to access this event.

Step 7: If the bidder is bidding for the first time for CCG through ARIBA site, then please "SignUP" by creating User Name and password as mentioned in Sign Up page. Please follow the process, as mentioned in the Sign-up page, during creation of User Name and password. Also,a simple one-page registration screen will open for first time users. All (*) marks are the mandatory field to be filled in.

Those who already have User Name and password for accessing ARIBA events, they can LOGIN using same User Name and password.

If bidder has got User name and password for their other customer, same will not be applicable for TPWODL/TPNODL/TPSODL

Step 8: You will be able to see the RFQ.

Step 9: After review and downloading of all documents click on **“Review Pre-requisites.”**

Step 10: Review and accept **“Bidder Agreement”.**

Step 11: You can see attached pdf tender document against clause no 1.1.1 (Introduction).

Step 12: Vendor must attach pdf version of technical bid in the relevant section/field/clauseand should not attach any priced document.

The price schedule is attached in relevant section/field/clause. The same must be downloaded and the price and tax details should be filled in the prescribed format. The same should be submitted on the Bidder's letter head with signature and seal of the authorized personnel of the Bidder. The PDF version of this price bid to be attached in the relevant section/field/clause. In the Price Bid, all the unit price and taxes & duties should be in the provided format. Put "0" (ZERO) in the fields wherever not applicable.

Step 13: After successfully putting Techno commercial offer and price part then click on **"Submit Entire Response."**

Note: Once user ID and password created, bidder can also login to ARIBA site through thefollowing URL:

https://service.ariba.com/Sourcing.aw/124997008/aw?awh=r&awssk=oxt0s1BN&dard=1

Annexure-A

Preferential norms for procurement from MSMEs registered in the State of Odisha

1) Tender Fees

To participate in the tender, MSMEs registered in the State of Odisha shall pay Rs.1,000/- including GST towards cost of tender paper.

2) Earnest Money Deposit (EMD)

EMD shall be exempted for MSME Bidders registered in the State of Odisha. However, the Bidder shall be barred from participating in the tendering process for a period of 2 years in case it backs-out post award of the contract.

3) Qualification Requirement for Open Tenders

Qualification Requirement of Financial Turnover for MSME registered in the State of Odisha shall be reduced to 20% of the existing criteria.

For experience, instead of relying on the volumes / value of earlier Supplies / Projects, assessment of the Bidder shall be done based on feedback from Customers. Past performance experience at Tata Power and its Group Companies shall supersede feedback from other Customers.

4) Reservation for MSME

It shall be mandatory to procure at least 20% of the total volume of the procurement from MSME registered in the State of Odisha (however, it shall not apply where goods/services are not available with the MSME), subject to matching L1 discovered prices and meeting technical specifications including quality requirements.

5) Performance Bank Guarantees

Performance Bank Guarantee for MSME registered in the State of Odisha shall be 25% of thevalue prescribed.

CONTENTS OF THE ENQUIRY

S. NO.	PARTICULARS
1.	Event Information
2.	Submission of Bid Documents
3.	Bid Opening & Evaluation process
4.	Evaluation Criteria
5.	Award Decision
6.	Order of Preference/Contradiction
7.	Post Award Contract Administration
8.	Specifications and Standards
9.	General Conditions of Contract
10.	Safety
Annexures	
I	Annexure I – Schedule of Items
II	Annexure II – Technical Specifications.
III	Annexure III – Schedule of Deviations
IV	Annexure IV – Schedule of Commercial Specifications
V	Annexure V – Document Check List
VI	Annexure VI – Acceptance Form for Participation in Reverse Auction Event
VII	Annexure VII – General Condition of Contract
VIII	Annexure VIII – Safety Policy and Safety Terms and Conditions
IX	Annexure IX - Environment & Sustainability Policy
X	Annexure X – Tata Code of Conduct (TCOC)

Definition & Introduction of Centralized Contracts Group

The Centralized Contracts Group (CCG) is a shared services group of all the 4 Discoms. (TPCODL, TPNODL, TPSODL & TPWODL) in Odisha. The contract finalized by CCG shall be used by 4 Discoms to execute the work.

1.0 Event Information

1.1. Scope of work

Bids are invited from interested Bidders for the **Supply, Installation, Testing & Commissioning of the Firewall software** as per the Technical Specification mentioned in this Tender document at the designated stores of TPNODL/TPWODL/TPSODL on "FOR basis".

1.2. Availability of Tender Documents

Please refer “Procedure to participate in the e-tender”.

1.3. Calendar of Events

(a)	Date of availability of tender documents on the websites of TPCODL/TPNODL/TPSODL/TPWODL	30.09.2023
(b)	Last date and time of Payment of Tender Fee	10.10.2023
(c)	Last Date of receipt of pre-bid queries if any	14.10.2023, 17:00 Hours
(d)	Last Date of Posting Consolidated replies to all the pre-bid queries as received	18.10.2023, 17:00 Hours
(e)	Last date and time of receipt of Bids	25.10.2023, 17:00 Hours

Note: In the event of last date specified for submission of bids and date of opening of bids is declared as a closed holiday for TPCODL’s office, the last date of submission of bids and date of opening of bids will be theday following working day at appointed times.

1.4 Mandatory documents required along with the Bid:

1.4.1 Tender Fee.
1.4.2 Proper authorization letter/ Power of Attorney to sign the tender on the behalf of bidder.
1.4.3 EMD of requisite value and validity

1.4.4 Copy of PAN, GST registration (In case any of these documents is not available with the bidder, sameto be explicitly mentioned in the 'Schedule of Deviations')

1.4.5 Requisite Documents for compliance to Qualification Criteria mentioned in Clause 1.7.

1.4.6 Acceptance of Specification, drawing with filled in GTP as per Annexure II.

1.4.7 Duly signed and stamped 'Schedule of Deviations' as per Annexure III on bidder's letter head.

1.4.8 Duly signed and stamped 'Schedule of Commercial Specifications' as per Annexure IV on bidder's letter head.

1.4.9 Duly filled in Annexure V and VI.

1.4.10 Duly filled format for furnishing the details of the supplies made as proof of experience.

Please note that in the absence of any of the above documents, the bid submitted by a bidder shall be liable for rejection.

1.5. Deviation from Tender

Normally, deviations to tender terms are not admissible and the bids with deviation are liable for rejection.Hence, the bidders are advised to refrain from taking any deviations on this Tender. Still in case of any deviations, all such deviations shall be set out by the Bidders, clause by clause in the 'Annexure III - Schedule of Deviations' and same shall be submitted as a part of the Technical Bid.

1.6. Right of Acceptance/Rejection

Bids are liable for rejection in absence of following documents:

i. EMD of requisite value and validity.
ii. Tender fee of requisite value.
iii. Price Bid as per the Price Schedule mentioned in Annexure I (BOQ)
iv. Necessary documents against compliance to Qualification Requirements mentioned at Clause 1.7 ofthis Tender Document.
v. Filled in Schedule of Deviations as per Annexure III.
vi. Filled in Schedule of Commercial Specifications as per Annexure IV.
vii. Signed and filled in Specification and GTP as per Annexure II.
viii. Duly filled and signed Annexure V and VI.
ix. Receipt of Bid within the due date and time.

CCG reserves the right to accept/reject any or all the bids without assigning any reason thereof.

1.7 Qualification Criteria

A. The average annual turnover requirement of the bidder shall be a minimum of Rs.20.0 Crore (average of best three Financial year out of five Financial years shall be considered - FY 18-19, FY 19-20, FY 20-21, FY 21-22 & FY22-23). Copy of audited Balance Sheet and P&L Account to be submitted in this regard. Qualification Requirement of Financial Turnover for MSME registered in the State of Odisha shall be reduced to 20% of the existing criteria.

B. The proposed firewall vendor must be in Leader's quadrant of Gartner Enterprise Firewall report of 2021 for last three years. The Bidder should furnish documentary evidence regarding this.

C. The bidder should either be an OEM for tendered equipment's or an authorized channel partner of OEM. Authorization Letter from OEM to be submitted in this regard. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM personnel only. All the compliances should be submitted in the Bidder's letter head.

D. The Bidder should be Company registered in India with its branch/alternate office at Odisha/Eastern region of India. The Bidder shall submit an undertaking with its complete office address, in this regard.

E. The Bidder should be a CMMI Level - 3 or CMMI Level - 5 company. An undertaking to be submitted in this regard.

F. The bidder should have executed similar works for cumulative 6 Crore INR during last 3 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder’s other customer.

G. The bidder must have all statutory compliance like valid PAN, GSTN etc. The bidder must submita copy of all these registrations.

1.8. Marketing Integrity

We have a fair and competitive marketplace. The rules for bidders are outlined in the General Condition of Contracts. Bidders must agree to these rules prior to participating. In addition to other remedies available, CCG reserves the right to exclude a bidder from participating in future markets due to the bidder’s violationof any of the rules or obligations contained in the General Condition of Contracts. A bidder who violates themarket place rules or engages in behavior that disrupts the fair execution of the marketplace, may result inrestriction of a bidder from further participation in the marketplace for a length of time, depending upon the seriousness of the violation. Examples of violations include, but are not limited to:

- Failure to honor prices submitted to the market place.
- Breach of terms as published in TENDER/NIT

1.9. Supplier Confidentiality

All information contained in this tender is confidential and shall not be disclosed, published, or advertised in any manner without written authorization from TPWODL/TPNODL/TPSODL. This includes all bidding information submitted to TPWODL/TPNODL/TPSODL. All tender documents remain the property of TPWODL/TPNODL/TPSODL, and all suppliers are required to return these documents to TPCODL upon request. Suppliers who do not honor these confidentiality provisions will be excluded from participating in future bidding events.

2.0 Evaluation Criteria

- The bids will be evaluated technically and on qualifying criteria of tender terms and conditions.
- The bids will be evaluated commercially on an individual item basis (all-inclusive lowest cost at itemlevel) for the complete tender as calculated in Schedule of Items [Annexure I].
- Bidder must mandatorily quote against each item of Schedule of Items *[Annexure I].* Failing to do so, CCG may reject the bids.

NOTE: *In case a new bidder is not registered with* TPWODL/TPNODL/TPSODL*, factory inspection and evaluation shall be carried out to ascertain bidder's manufacturing capability and quality procedures. However,* TPWODL/TPNODL/TPSODL *reserves the right to carry out factory inspection and evaluation for any bidder prior to technical qualification.*

In case a bidder is found as Disqualified in the factory evaluation, their bid shall not be evaluated any furtherand shall be summarily rejected. The decision of TPWODL/TPNODL/TPSODL *shall be final and binding on the bidder in this regard.*

2.1 Price Basis: Price will be fixed and firm during the contractual period.

3.0 Submission of Bid Documents.

3.1 Bid Submission

Bidders are requested to submit their offer in line with this Tender document through e-tendering process.

Please note all future correspondence regarding the tender, bid submission, bid submission date extension,Pre-bid query etc. will happen only through E-Tender system (Ariba).

No e-mail or verbal correspondence will be responded. All communication will be done strictly with the bidder who has done the above step to participate in the Tender.

Bids shall be submitted in 3(Three) parts:

FIRST PART: "EMD" as applicable shall be submitted. The EMD shall be valid for 210 days from the due dateof bid submission in the form of Bank Guarantee / Bank Draft / Bankers Pay Order (issued from a ScheduledBank) online NEFT/ RTGS transfer favoring 'TP Central Odisha Distribution Limited' payable at Bhubaneswar.The EMD BG must be strictly in the format as mentioned in the General Condition of Contract, failing which it shall not be accepted by CCG and the bid as submitted shall be liable for rejection. A separate non- refundable tender fee of the stipulated amount also needs to be transferred online through NEFT/ RTGS in case the tender document is downloaded from our website.

TPCODL Bank Details for transferring Tender Fee and EMD is as below:

Account Name: TP CENTRAL ODISHA DISTRIBUTION LIMITED
Bank Name: SBI, IDCO Towers, Bhubaneswar
Bank Account No.: 10835304915
IFSC Code: SBIN0007891

Note: EMD is preferred in the form of Bank Guarantee and to be delivered at the following address. However, in view of the present situation if Bidder is finding it difficult to make and submit BG for EMD amount, they can do online transfer of EMD amount in the above-mentioned Account and submit proof of the same as part of Bid Submission.

Please note that in such a case, Tender Fee and EMD should be strictly 2 separate transactions.

Please note as return of EMD from Bank Account is non-standard practice and the same may take more timethan return of EMD BG.

EMD Original Hard Copy shall be delivered at the following address in Envelope clearly indicating Tender Reference/ Enquiry Number, Name of Tender and Bidder Name

Chief – Centralized Contracts Group
TP Central Odisha Distribution Limited
1st Floor, Anuj Building, Plot No. 29, Satya Nagar, Bhubaneswar- 751007

EMD shall be exempted from MSME registered in the State of Odisha. However, Bidder shall be barred to participate in the tendering process for a period of 2 years in case it backs out post award of the contract.

SECOND PART: "TECHNICAL BID" shall contain the following documents:

i) Requisite Documents for compliance with Qualification Criteria mentioned in Clause 1.7 and clause no.1.4.
ii) Type Test Certificate of Lightning Arrester of same or higher rating.
iii) Acceptance of Specification as per Annexure II.
iv) Duly signed and stamped 'Schedule of Deviations' as per Annexure III on bidder's letter head.
iv) Duly signed and stamped 'Schedule of Commercial Specifications' as per Annexure IV on bidder's letterhead.
v) Duly filled in Annexure V and VI.
vi) Proper authorization letter/ Power of Attorney to sign the tender on the behalf of bidder.
vii) Copy of PAN, GST registration (In case any of these documents is not available with the bidder, same tobe explicitly mentioned in the 'Schedule of Deviations')

The technical bid shall be properly indexed and is to be submitted through CCG's E-tender System (Ariba)only. Hard Copy of Technical Bids need not be submitted.

THIRD PART: "PRICE BID" shall contain only the price details and strictly in format as mentioned in AnnexureI along with explicit break up of basic prices and Taxes & duties etc. In case any discrepancy is observed between the item description stated in the Schedule of Items mentioned in the tender and the price bid submitted by the bidder, the item description as mentioned in the tender document (to the extent modifiedthrough Corrigendum issued if any) shall prevail.

Price Bid is to be submitted in soft copy through CCG E-Tendering system (Ariba) only. Hard copy of Price Bid not to be submitted.

The EMD in the form of Bank Draft / BG / Bankers Pay Order shall be submitted in original hard copy and then placed in sealed envelope which shall be clearly marked as below:

EMD

"Supply, Installation, Testing & Commissioning of the Firewall software" The Bid prepared by the Bidder, and all correspondence and documents relating to the Bid exchanged by the Bidder and the CCG, shall be written in the English Language. Any printed literature furnished by the Bidder may be written in another Language, provided that this literature is accompanied by an English translation, in which case, for purposes of interpretation of the Bid, the English translation shall govern.

SIGNING OF BID DOCUMENTS:

The bid must contain the name, residence, and place of business of the person or person making the bid and must be signed and sealed by the Bidder with his usual signature. The names of all the people signing should also be typed or printed below the signature.

The Bid being submitted must be signed by a person holding a Power of Attorney authorizing him to do so,certified copies of which shall be enclosed.

The Bid submitted on behalf of companies registered with the Indian Companies Act, for the time being in force, shall be signed by persons duly authorized to submit the Bid on behalf of the Company and shall be accompanied by certified true copies of the resolutions, extracts of Articles of Association, special or general Power of Attorney etc. to show clearly the title, authority and designation of persons signing the Bid on behalf of the Company. Satisfactory evidence of authority of the person signing on behalf of the Bidder shallbe furnished with bid.

A bid by a person who affixes to his signature the word 'President', 'Managing Director', 'Secretary', 'Agent' or other designation without disclosing his principal will be rejected.

The Bidder's name stated on the Proposal shall be the exact legal name of the firm.

3.2 Contact Information

All the bidders are requested to send their pre-bid queries (if any) against this tender through e-mail withinthe stipulated timelines. The consolidated reply to all the queries received shall be posted on TPCODL/TPNODL/TPSODL/TPWODL website within the stipulated timelines as detailed in calendar of events.

Communication Details:

Package owner:

Name: Saurabh Kumar
Contact No.: 7004418500
E-Mail ID: saurabh.kumar@tpwesternodisha.com

Head -CCG:

Name: Mr. Vipin Chauhan
Contact No.: 9717393121
E-Mail ID: vipin.Chauhan@tpnodl.com

3.3 Bid Prices

Bidders need to quote for all items as per the Price schedule attached in Annexure I. The bidder shall complete the appropriate Price Schedules included herein, stating the Unit Price for each item & total pricewith taxes, duties & freight up to destination at various sites of TPWODL/TPNODL/TPSODL. The all-inclusive prices offered shall be inclusive of all costs as well as Duties, Taxes and Levies paid or payable during the execution of the supply work, breakup of price constituents.

Applicable GST to be specified clearly.

The quantity break-up shown elsewhere other than the Price Schedule is tentative. The bidder shall ascertain himself regarding material required for completeness of the entire work. Any items not indicated in the price schedule, but which are required to complete the job as per the Technical Specifications/ Scope of Work/ SLA mentioned in the tender, shall be deemed to be included in prices quoted.

3.4 Bid Currencies

Prices shall be quoted in Indian Rupees Only.

3.5 Period of Validity of Bids

Bids shall remain valid for 180 days from the due date of submission of the bid.

Notwithstanding clause above, the TPWODL/TPNODL/TPSODL may solicit the Bidder's consent to
an extension of the Period of Bid Validity. The request and responses thereto shall be made in writing.

3.6 Alternative Bids

Bidders shall submit Bids, which comply with the Bidding documents. Alternative bids will not be considered. The attention of Bidders is drawn to the provisions regarding the rejection of Bids in the terms and conditions, which are not substantially responsive to the requirements of the bidding documents.

3.7 Modifications and Withdrawal of Bids

The bidder is not allowed to modify or withdraw its bid after the Bid's submission. The EMD as submitted along with the bid shall be liable for forfeiture in such an event.

3.8 Earnest Money Deposit (EMD)

The bidder shall furnish, as part of its bid, an EMD amounting as specified in the tender. The EMD is required to protect CCG against the risk of bidder's conduct which would warrant forfeiture.

The EMD shall be denominated in any of the following form:

- Banker's Cheque/ Demand Draft/ Pay order drawn in favor of TP Central Odisha Distribution Limited payable at Bhubaneswar.
- Online transfer of requisite amount through NEFT/ RTGS.
- Bank Guarantee valid for 210 days after the due date of submission.

The EMD shall be forfeited in case:

a) The bidder withdraws its bid during the period of specified bid validity.

Or

b) The successful Bidder does not
   a) accept the Purchase Order, or
   b) furnish the required Performance Security Bank Guarantee.

3.9 Type Tests (if applicable).

The type tests specified in TPNODL/TPSODL/TPWODL specifications should have been carried out within five years prior to the date of opening of technical bids and test reports are to be submitted along with thebids. If type tests carried out are not within the five years prior to the date of bidding, the bidder will arrange to carry out type tests specified, at his cost. The decision to accept/ reject such bids rests with TPCODL/TPNODL/TPSODL/TPWODL.

4 Bid Opening & Evaluation process.

4.1. Process to be confidential.

Information relating to the examination, clarification, evaluation and comparison of Bids and recommendations for the award of a contract shall not be disclosed to Bidders or any other persons not officially concerned with such process. Any effort by a Bidder to influence the TPWODL/TPNODL/TPSODL processing of Bids or award decisions may result in rejection of the Bidder's Bid.

4.2. Technical Bid Opening

Bids will be opened at CCG Office, Bhubaneswar. All tender bids shall be opened internally by CCG. The presence of any bidder will not be allowed during the bid opening process. A technical bid must not contain any cost information whatsoever.

First the envelope marked “EMD” will be opened. Bids without EMD/cost of tender (if applicable) of requiredamount/ validity in prescribed format, shall be rejected.

Next, the technical bid of the bidders who have furnished the requisite EMD will be opened, one by one.

4.3. Preliminary Examination of Bids/Responsiveness

CCG will examine the Bids to determine whether they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed, and whether the Bids are generally in order. CCG may ask for submission of original documents to verify the documents submitted in support of qualification criteria.

Arithmetical errors will be rectified on the following basis: If there is a discrepancy between the unit price and the total price per item that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price per item will be corrected. If there is a discrepancy between the Total Amount and the sum of the total price per item, the sum of the total price per item shall prevail and the Total Amountwill be corrected.

Prior to the detailed evaluation, CCG will determine the substantial responsiveness of each Bid to the Bidding Documents including production capability and acceptable quality of the Goods offered. A substantially responsive Bid is one which conforms to all the terms and conditions of the Bidding Documentswithout material deviation.

Bids determined as not substantially responsive will be rejected by the TPWODL/TPNODL/TPSODL and may not subsequently be made responsive by the Bidder by correction of the non-conformity.

4.4. Techno Commercial Clarifications

Bidders need to ensure that the bids submitted by them are complete in all respects. To assist in the examination, evaluation, and comparison of Bids, TPWODL/TPNODL/TPSODL may, at its discretion, ask the Bidder for a clarification on its Bid for any deviations with respect to the TPWODL/TPNODL/TPSODLspecifications and attempt will be made to bring all bids on a common footing. All responses to requests for clarification shall be in writing and no change in the price or substance of the Bid shall be sought, offered, or permitted owing to any clarifications sought by TPWODL/TPNODL/TPSODL.

4.5. Price Bid Opening

Price bids will be opened internally without the presence of any bidder representative. The EMD of the bidder withdrawing or substantially altering his offer at any stage after the technical bid opening will be forfeited at the sole discretion of TPWODL/TPNODL/TPSODL without any further correspondence in this regard.

4.6. Reverse Auctions

CCG reserves the right to conduct a reverse auction (instead of public opening of price bids) for the products/ services being asked for in the tender. The terms and conditions for such reverse auction events shall be as per the Acceptance Form attached as Annexure VI to this document. The bidders along with the tender document shall mandatorily submit a duly signed copy of the Acceptance Form attached as AnnexureVI as a token of acceptance for the same.

5 Award Decision

CCG will award the contract to the successful bidder whose bid has been determined to be the lowest- evaluated responsive bid as per the Evaluation Criterion mentioned at Clause 2.0. The Cost for the said calculation shall be taken as the all-inclusive cost quoted by bidder in Annexure I (Schedule of Items) subjectto any corrections required in line with Clause 3.1 above. The decision to place purchase order/LOI solely depends on CCG on the cost competitiveness across multiple lots, quality, delivery, and bidder’s capacity, inaddition to other factors that CCG may deem relevant.

CCG reserves the right to award contracts to one or more bidders to meet the delivery requirement or nullify the award decision without assigning any reason thereof.

In case any supplier is found unsatisfactory during the delivery process, the award will be cancelled, and CCG reserves the right to award contracts to other suppliers who are found fit.

6 Order of Preference/Contradiction

In case of contradiction in any part of various documents in tender, following shall prevail in order of preference:

1. Schedule of Items (Annexure I)
2. Technical Specifications (Annexure II)
3. Special Conditions of Contract (Clause 7.0)
4. Submission of Bid Documents (Clause 3.0)
5. Acceptance Form for Participation in Reverse Auction (Annexure VI)
6. General Conditions of Contract (Annexure VIII)

7 Post Award Contract Administration

7.1. Special Conditions of Contract

a) The Rate Contract (RC) shall be valid for a period of 1 (one) year from the placement of Contract. ReleaseOrder (RO) shall be issued as per the requirement of TPSODL/TPWODL/TPNODL. The rate shall be firm and fixed during the validity of the contract.

b) The Business Associate (BA) shall submit applicable Performance Bank Guarantee (PBG) as per GCC within 30 days of issuance of purchase order. PBG applicable shall be @ 5% of Rate Contract Value havinga validity till warranty period plus one month.

c) Any change in statutory taxes, duties and levies during the contract period shall be borne by TPSODL/TPWODL/TPNODL. However, in case of delay in work execution owing to reasons not attributable to TPSODL/TPWODL/TPNODL, any increase in total liability shall be passed on the Bidder, whereas any benefits arising owing to such statutory variation in taxes and duties shall be passed on TPSODL/TPWODL/TPNODL.

d) Statutory Variations: Any changes in existing taxes/ Duties and levies, Introduction of new taxes and duties etc. during the period of the contract shall be paid at actuals to BA subject to BA shall submit the tax break up in details, however, where BA has quoted the all-inclusive prices and not shown the tax break-up, this clause will not be applicable. The date of issue of MDCC shall be used for this purpose.

e) Quotation in all BOQ items is mandatory, and bid shall be rejected if any line of found blank in price bid.

f) Delivery period shall be 60 days from date of receipt of Release Order / CAT-A GTP approval, whichever is later.

g) Warranty period: The Bidder shall provide a warranty on the Firewall software with total support from OEM, for a period of 5 years from the date of the commissioning of the software.

h) Delivery location: As per the instruction from the Engineer In-charge.

i) The Liquidated Damages (LD) shall be applicable as per GCC.

j) All other terms and conditions mentioned in the General Conditions of Contract shall be applicable.

k) TPCODL /TPWODL shall short close the issued Purchase Order/ Release Order / Rate contract,in case of any quality issues

l) Terms of Payment:

a. **<u>Supply part:</u>** On delivery of the software complete in all respect and certification of acceptance by certified official, Associate shall submit the Bills/ Invoices in original along with all the requisite documents, in the name of TP Central Odisha Distribution Limited to Invoice Desk. The payment a payment of 60% of the Invoice basic value along with 100% tax as applicable, shall be made within 90 days of the submission of the invoices along with all the requisite documents However, for MSME Bidders, the payment shall be released within 45 days of the submission of the bills/invoice.

b. **<u>Installation, Testing & Commissioning:</u>** Upon Installation, Testing & Commissioning of the software complete in all respect and certification of acceptance by certified official, Associate shall submit the Bills/ Invoices in original along with all the requisite documents, in the name of TP Central Odisha Distribution Limited to Invoice Desk. The payment a payment of balance 40% of the Invoice basic value along with 100% tax as applicable, shall be made within 90 days of the submission of the invoices along with all the requisite documents. However, for MSME Bidders, the payment shall be released within 45 days of the submission of the bills/invoice.

7.2 Architecture Submission and Approval

The relevant architecture, if applicable, should be submitted within 15 days of receipt of the Rate Contract by the successful bidder, for approval. In case re-submission of drawings is required, the same needs shall besubmitted within 5 days of such request.

7.3 Payment Terms

As per SCC, Clause number 7.1 (l).

7.4 Climate Change

Significant quantities of waste are generated during the execution of a project and an integrated approach for effective handling, storage, transportation, and disposal of the same shall be adopted. This would ensure the minimization of environmental and social impact to combat climate change. Please refer to the attached Environment Policy and Sustainability Policy, enclosed for more details.

7.5 Ethics

TPSODL/TPNODL/TPWODL is an ethical organization and as a policy TPSODL/TPNODL/TPWODL lays emphasis on ethical practices across its entire domain. Bidder should ensure that they should abide by all the ethical norms and in no form either directly or indirectly be involved in unethical practice.

CCG work practices are governed by the Tata Code of Conduct which emphasizes on the following:

a) We shall select our suppliers and service providers fairly and transparently.

b) We seek to work with suppliers and service providers who can demonstrate that they share similar values. We expect them to adopt ethical standards comparable to our own.

c) Our suppliers and service providers shall represent our company only with duly authorized written permission from our company. They are expected to abide by the Code in their interactions with, and on behalf of us, including respecting the confidentiality of information shared with them.

d) We shall ensure that any gifts or hospitality received from, or given to, our suppliers or service providerscomply with our company's gifts and hospitality policy.

e) We respect our obligations on the use of third-party intellectual property and data.Bidder

is advised to refer Tata Code of Conduct (TCOC) attached for more information.

Any ethical concerns with respect to this tender can be reported to the following e-mail ID: pradip.sil@tpcentralodisha.com.

8 Specification and standards

As per Annexure II

9 General Condition of Contract

Any condition not mentioned above shall be applicable as per the GCC attached along with this tender.

ANNEXURE-I

Sl. No.	Description	UoM	TPCODL	TPWODL	Unit Rate	GST@ 18%	Total Price
1	**SITC of DC/DR Internal Firewall with Perpetual License including 05-year OEM Warranty and Premium Support**						
1.1	SITC for Fully Populated Internal Firewall v1.0 in HA with 5 Yrs. Support -FOR Central DR INFRUSTRUCTRE (2 Firewall, 01 Analyzer, 8 x 100G SR SFP, 24 X 25G SR SFP, 16 x GE SFP SR SFP, 32 x GE RJ45 Ports, 4 x GE RJ45 MGMT Ports, 4 x 10 GE SFP+ / GE SFP HA Slots with SFP)	Solution	0	1			
1.2	SITC for Fully Populated Internal Firewall v1.1 in HA with 5 Yrs. Support -FOR Individual DC/DR INFRUSTRUCTRE (2 Firewall, 01 Analyzer, 8 x 100G SR SFP, 24 X 10G SR SFP, 16 x GE SFP SR SFP, 32 x GE RJ45 Ports, 4 x GE RJ45 MGMT Ports, 4 x 10 GE SFP+ / GE SFP HA Slots with SFP)	Solution	0	1			
2	**SITC of DC/DR Perimeter Firewall with Perpetual License including 05-year OEM Warranty and Premium Support**						
2.1	SITC OF Perimeter Firewall v1.0 in HA and One Management Box with 5 Yrs. Support- FOR Central DR INFRUSTRUCTRE (Around 300 Gb FW Throughput, 154 Gb NGFW Throughput, 150 Gb IPS Throughput, 90 Gb Threat Prevention throughput)	Solution	0	1			
2.2	SITC OF Perimeter Firewall v1.1 in HA along One Management Box/ virtual appliance, one sandbox appliance and firewall analyzer with 5 Yrs. Support- For Individual DC/DR INFRUSTRUCTRE DC-DR Perimeter Firewall-v1.2 must follow.	Solution	1	0			
3	**SITC OF Perimeter Sandboxing in HA with 5 Yrs. OEM Premium Support- For Individual DC/DR INFRUSTRUCTRE** (Minimum 2 Gb Sandboxing, 28 Virtual Machines, 2200 unique files/hour, 100 Mb max File size, Zero Day protection, 5 Yrs. OEM Warranty and Premium Support)	Solution	0	1			

Note:

- The overall period of the rate contract shall be of One Year and prices shall remain firm till the validity of the contract. Release order shall be issued as per the requirement.
- The bidders are advised to quote prices strictly in the above format. Failing to do so, bids shall be liable for rejection.
- Bidder needs to quote mandatorily, for each line item of the BOQ.
- The Bidder should mention the HSN code of the items as indicated in the above Annexure-1 table.
- The bidder must fill each column of the above format. Mentioning “extra/inclusive” in any of the columns maylead to rejection of the price bid.
- No cutting/ overwriting in the prices is permissible.

ANNEXURE II

Detailed Scope of Work: Appended

ANNEXURE III

Schedule of Deviations

Bidders are advised to refrain from taking any deviations on this TENDER. Still in case of any deviations, all such deviations from this tender document shall be set out by the Bidders, Clause by Clause in this scheduleand submit the same as a part of the ***Technical Bid.***

Unless <u>specifically</u> mentioned in this schedule, the tender shall be deemed to confirm the TPWODL/TPNODL/TPSODL***'s specifications:***

Sl. No.	Clause No.	Tender Clause Details	Details of deviation with justifications

By signing this document, we hereby withdraw all the deviations whatsoever taken anywhere in this bid document and comply to all the terms and conditions, technical specifications, scope of work etc. as mentioned in the standard document except those as mentioned above.

Seal of the Bidder:

Signature:

Name:

ANNEXURE IV

Schedule of Commercial Specifications

(The bidders shall mandatorily fill in this schedule and enclose it with theoffer Part I: Technical Bid. In theabsence of all these details, the offer may not be acceptable.)

Sl. No.	Particulars	Remarks
1.	Prices firm or subject to variation (If variable indicate the price variation clause with the ceiling if applicable)	Firm / Variable
1a.	If variable price variation on clause given	Yes / No
1b.	Ceiling	--------- %
1c.	Inclusive of GST	Yes / No (If Yes, indicate % rate)
1d.	Inclusive of transit insurance	Yes / No
2.	Delivery	Weeks / months
3.	Guarantee clause acceptable	Yes / No
4.	Terms of payment acceptable	Yes / No
5.	Performance Bank Guarantee acceptable	Yes / No
6.	Liquidated damages clause acceptable	Yes / No
7.	Validity (180 days) (From the date of opening of bid)	Yes / No
8.	Inspection during stage of manufacture	Yes / No
9.	Rebate for increased quantity (If Yes, indicate value)	Yes / No
10.	Change in price for reduced quantity	Yes / No (If Yes, indicate value)
11.	Covered under Small Scale and Ancillary Industrial Undertaking Act 1992	Yes / No (If Yes, indicate, SSI Reg'n No.)

Seal of the Bidder:

Signature:

Name:

ANNEXURE V

Checklist of all the documents to be submitted with the Bid.

Bidder must mandatorily fill in the checklist mentioned below:

S. No.	Documents attached	Yes / No / Not Applicable
1	EMD of required value	
2	Tender Fee as mentioned in this tender	
3	Signed copy of this tender as an unconditional acceptance	
5	Duly filled schedule of commercial specifications (Annexure IV)	
6	Sheet of commercial/technical deviation if any (Annexure III)	
7	Balance sheet for the last completed three financial years; mandatorily enclosing Profit & loss account statement	
8	Acknowledgement for Testing facilities if available (duly mentioned onbidder letter head)	
9	List of Machine/tools with updated calibration certificates if applicable	
10	Details of order copy (duly mentioned on bidder letter head)	
11	Order copies as a proof of quantity executed	
12	Details of Type Tests if applicable (duly mentioned on bidder letter head)	
13	All the relevant Type test certificates as per relevant IS/IEC (CPRI/ERDA/other certified agency) if applicable	
14	Project/supply Completion certificates	
15	Performance certificates	
16	Client Testimonial/Performance Certificates	
17	Credit rating/solvency certificate	
18	Undertaking regarding non blacklisting (On company letter head)	
19	List of trained/untrained Manpower	

Seal of the Bidder:

Signature:

Name

ANNEXURE VI

ACCEPTANCE FORM FOR PARTICIPATION IN REVERSE AUCTION EVENT

(To be signed and stamped by the bidder)

In a bid to make our entire procurement process fairer and more transparent, CCG intends to use the reverse auctions as an integral part of the entire tendering process. All the bidders who are found technicallyqualified based on the tender requirements shall be eligible to participate in the reverse auction event.

The following terms and conditions are deemed as accepted by the bidder on participation in the bid event:

1. TPWODL/TPNODL/TPSODL shall provide the user id and password to the authorized representative of the bidder. *(Authorization Letter in lieu of the same shall be submitted along with the signed and stamped Acceptance Form).*

2. TPWODL/TPNODL/TPSODL will make every effort to make the bid process transparent. However, the award decision by TPWODL/TPNODL/TPSODL would be final and binding on the supplier.

3. The bidder agrees to non-disclosure of trade information regarding the purchase, identity of TPWODL/TPNODL/TPSODL, bid process, bid technology, bid documentation, and bid details.

4. The bidder is advised to understand the auto bid process to safeguard themselves against any possibilityof non-participation in the auction event.

5. In case of bidding through Internet medium, bidders are further advised to ensure availability of the entire infrastructure as required at their end to participate in the auction event. Inability to bid due to telephone line glitch, internet response issues, software or hardware hangs, power failure or any otherreason shall not be the responsibility of TPWODL/TPNODL/TPSODL.

6. In the case of intranet medium, TPWODL/TPNODL/TPSODL shall provide the infrastructure to bidders. Further, TPWODL/TPNODL/TPSODL has sole discretion to extend or restart the auction event in case of any glitches in infrastructure observed which has restricted the bidders from submitting the bids to ensure fair & transparent competitive bidding. In case an auction event is restarted, the best bid as already available in the system shall become the start price for the new auction.

7. In case the bidder fails to participate in the auction event due any reason whatsoever, it shall be presumed that the bidder has no further discounts to offer, and the initial bid as submitted by the bidderas a part of the tender shall be considered as the bidder's final no regret offer. Any offline price bids received from a bidder in lieu of non-participation in the auction event shall be outrightly rejected by TPWODL/TPNODL/TPSODL.

8. The bidder shall be prepared with competitive price quotes on the day of the bidding event.

9. The prices as quoted by the bidder during the auction event shall be inclusive of all the applicable taxes, duties and levies and shall be FOR at TPCODL/TPSODL/TPNODL/TPWODL site.

10. The prices submitted by a bidder during the auction event shall be binding on the bidder.

11. No requests for time extension of auction event shall be considered by TPWODL/TPNODL/TPSODL.

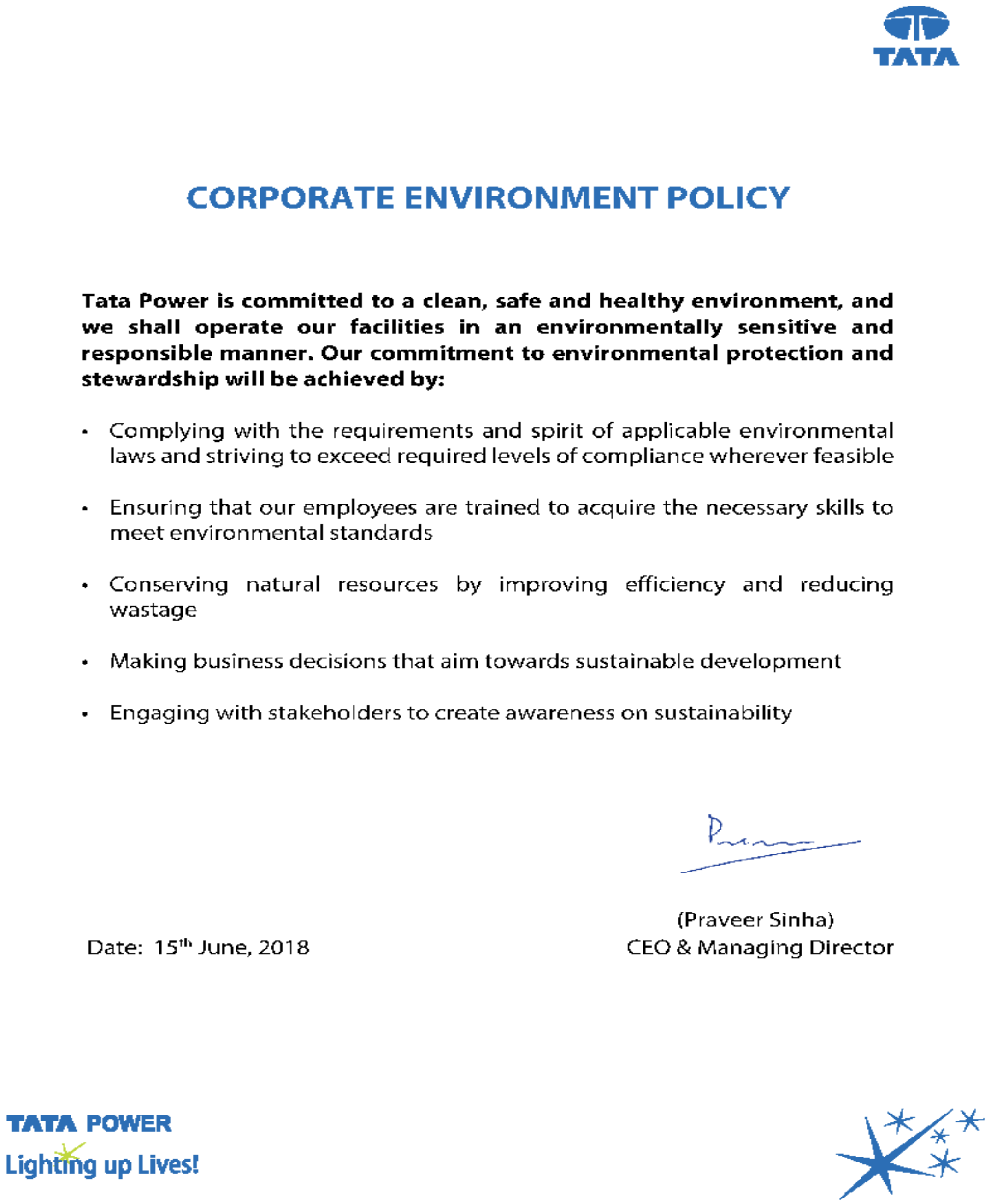
12. The original price bids of the bidders shall be reduced on a pro-rata basis against each line item based on the final all-inclusive prices offered during conclusion of the auction event for arriving at Contract amount.

ANNEXURE VII

General Conditions of Contract (GCC) for TPCODL, TPNODL, TPSODL and TPWODL: Annexed separately.

ANNEXURE - VIII: **Safety Policy and Safety Terms and Conditions:** Attached separately.

ANNEXURE - IX: ENVIRONMENT & SUSTAINABILITY POLICY



TATA

CORPORATE ENVIRONMENT POLICY

Tata Power is committed to a clean, safe and healthy environment, and we shall operate our facilities in an environmentally sensitive and responsible manner. Our commitment to environmental protection and stewardship will be achieved by:

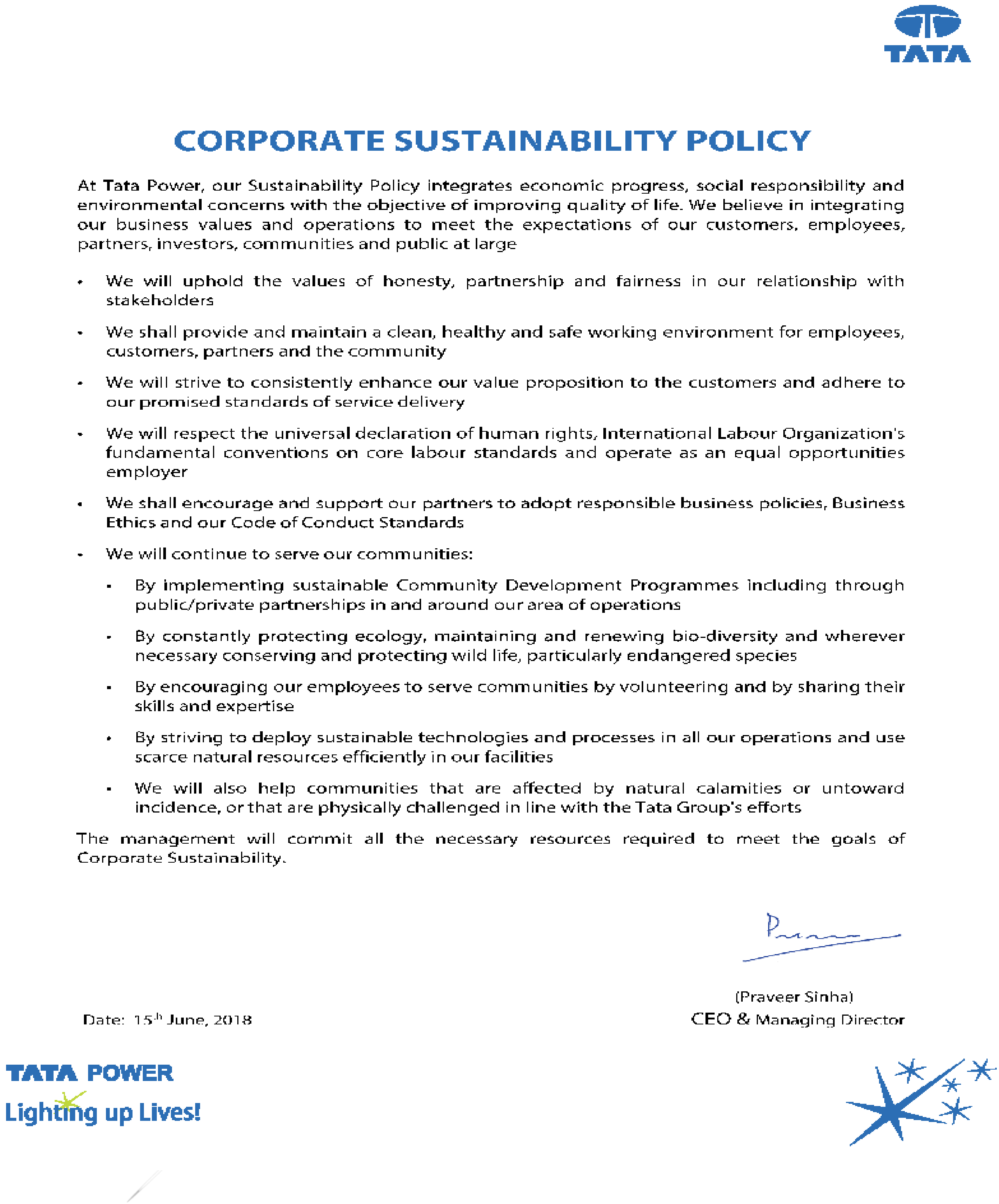
- Complying with the requirements and spirit of applicable environmental laws and striving to exceed required levels of compliance wherever feasible
- Ensuring that our employees are trained to acquire the necessary skills to meet environmental standards
- Conserving natural resources by improving efficiency and reducing wastage
- Making business decisions that aim towards sustainable development
- Engaging with stakeholders to create awareness on sustainability

(Praveer Sinha)
CEO & Managing Director

Date: 15th June, 2018

TATA POWER
Lighting up Lives!

ANNEXURE - X:



TATA

CORPORATE SUSTAINABILITY POLICY

At Tata Power, our Sustainability Policy integrates economic progress, social responsibility and environmental concerns with the objective of improving quality of life. We believe in integrating our business values and operations to meet the expectations of our customers, employees, partners, investors, communities and public at large

- We will uphold the values of honesty, partnership and fairness in our relationship with stakeholders
- We shall provide and maintain a clean, healthy and safe working environment for employees, customers, partners and the community
- We will strive to consistently enhance our value proposition to the customers and adhere to our promised standards of service delivery
- We will respect the universal declaration of human rights, International Labour Organization's fundamental conventions on core labour standards and operate as an equal opportunities employer
- We shall encourage and support our partners to adopt responsible business policies, Business Ethics and our Code of Conduct Standards
- We will continue to serve our communities:
  - By implementing sustainable Community Development Programmes including through public/private partnerships in and around our area of operations
  - By constantly protecting ecology, maintaining and renewing bio-diversity and wherever necessary conserving and protecting wild life, particularly endangered species
  - By encouraging our employees to serve communities by volunteering and by sharing their skills and expertise
  - By striving to deploy sustainable technologies and processes in all our operations and use scarce natural resources efficiently in our facilities
  - We will also help communities that are affected by natural calamities or untoward incidence, or that are physically challenged in line with the Tata Group's efforts

The management will commit all the necessary resources required to meet the goals of Corporate Sustainability.

(Praveer Sinha)
CEO & Managing Director

Date: 15th June, 2018

TATA POWER
Lighting up Lives!

Technical Specification for 'DR INTERNAL FIREWALL-v1.0'

SL. no	Specification Minimum Required	Compliance Yes / No	Remarks
1.1	The proposed firewall vendor must be in Leader's quadrant of Gartner Enterprise Firewall report of 2021 for last three years		
1.2	The Firewall should be fixed Hardware based, Reliable, purpose-built security appliance with hardened operating system supporting State full policy inspection technology.		
Solution General Description			
2.1	The proposed solution shall have built-in high availability (HA) features without extra cost/license or hardware component		
2.2	The Solution must be supported both Active-Passive and Active-Active High Availability options		
2.3	The Solution must be deployed in Active-Active High Availability options.		
2.4	The Solution must be deployed in Full-Mesh		
2.5	The Solution must be supported and deployed in IPv4-IPv6 Dual Stack		
Firewall General Description			
3.1	Each Firewall appliance of the Solution must have 2 x GE RJ45 MGMT Ports, 2 x 10 GE SFP+ / GE SFP, HA Slots, 16 x GE RJ45 Ports, 8 x GE SFP Slots, 12 x 25 SFP28 / 10 GE SFP+/ GE SFP Slots, 4 x 100 GE QSFP28 / 40 GE QSFP+ Slots interfaces from day one. All these interfaces should be available simultaneously.		
3.2	Each Firewall appliance of the Solution must have minimum 4 x 100 Gbe Ethernet Ports along with 8 x 25G ports from day-1 excluding Management and HA interface. Single Mode SFP (Fiber/Copper) for all ports needs to be provide		
3.3	Each Firewall appliance of the Solution must be rack mountable & have hot swappable dual power supply		
4	Each Firewall appliance of the Solution FW throughput should be at least 140 Gbps		
5	Each Firewall appliance of the Solution Threat Prevention (including FW, IPS, Application Control & Antivirus) throughput must be at least 15 Gbps with real-world / enterprise MIX traffic		
6	Each Firewall appliance of the Solution NGFW (including FW, IPS, Application Control) throughput must be at least 17 Gbps with real-world / enterprise MIX traffic		
7	Each Firewall appliance of the Solution NGFW should have IPsec VPN throughput of at least 55 Gbps		
8	Each Firewall appliance of the Solution NGFW should support 20000 site-to-site VPN Tunnels.		
9	Each Firewall appliance of the Solution NGFW should support more than 750000 new sessions per second		
10	Each Firewall appliance of the Solution should support at least 12 Million concurrent sessions		
11	The vendor must have a security gateway solution that can support the enablement of all next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus.		
12	Each Firewall appliance of the Solution should not introduce more than 3.22 microsecond latency. Vendor's claim must be available in publicly available documents like datasheet, admin guide etc. Claim on company's letterhead		

	will not be acceptable.		
13	Each Firewall appliance of the Solution should support NAT64, NAT46, DNSv6 & DHCPv6		
14	The proposed system should be able to operate in Transparent (Access) mode and NAT/Route mode simultaneously without creating virtual context or virtual firewall		
15	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard, allowing the grouping of interfaces into a larger bandwidth 'trunk'. It should also allow for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk. NGFW should support ASIC based hardware,		
16	The NGFW should support WAN links load balancing and fail-over for at least 4 links		
17	The NGFW should support internet links load balancing and fail-over based parameters such as Latency, Jitter, Packet-Loss,		
18	The proposed system should have integrated Traffic Shaping functionality for both inbound and outbound traffic.		
19	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN) with minimum 10 Virtual Firewall license. And SD-WAN enabled from Day 1, all bandwidth cost should be provided from Day 1,		
20	The Firewall & IPSEC VPN module should have ICSA or other equivalent Certification.		
21	The NGFW should have both SSL and SSH Inspection capabilities		
22	The system should support 2 forms of site-to-site VPN configurations:		
23	a) Route based IPsec tunnel		
24	b) Policy based IPsec tunnel		
25	The system should support IPSEC site-to-site VPN and remote user IPsec VPN in transparent mode.		
26	The system should provide IPv6 IPsec feature to support for secure IPv6 traffic in an IPsec VPN.		
27	Solution must support at least 10 Gbps SSL-VPN Throughput		
28	The proposed firewall must support at least 10 Gbps of SSL Inspection throughput along with IPS feature enabled.		
29	Proposed NGFW must not require reboot to push security policies or any signature (IPS, Anti-malware etc.) update.		
30	The NGFW shall be able to support various form of user Authentication methods simultaneously, including Local Database, LDAP, RADIUS, TACACS+, Windows AD, Citrix & Terminal Server Agent support for Single Sign On		
31	The NGFW should readily available integration with SDN platforms - Kubernetes, VMware ESXi and NSX, OpenStack, Cisco ACI, Nuage Networks and Nutanix		
Intrusion Prevention System			
31	Each Firewall appliance of the Solution IPS throughput should be at least 22 Gbps or better for Enterprise MIX traffic		
32	Each Firewall appliance of the Solution IPS should be able to inspect SSL sessions by decrypting the traffic		
33	Each Firewall appliance of the Solution IPS system should have at least 11,000 signatures		

34	In event if IPS should cease to function, it should fail open by default and be configurable so that crucial network traffic should not be blocked and NGFW should continue to operate while the IPS problem is being resolved		
35	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 lookups.		
36	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g., for severity level: high medium low)		
37	NGFW 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.		
Application Control Features:			
38	Each Firewall appliance of the Solution should have at least 4000 application signatures database		
39	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.		
40	Firewall must have capability to do Cloud application-based routing not by means of manually adding IPs and or FQDNs i.e. firewall should have database of O365 readily available to select as destination address in firewall policy and destination address in static route configuration to give particular ISP path		
Anti-Malware & Advanced Persistent Threat			
41	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 and their equivalent encrypted versions, wherever applicable: HTTP, SMTP, POP3, IMAP, FTP, CIFS, NNTP, SSH, MAPI		
42	NGFW should offer both anti-viruses scanning options - Proxy mode and Flow (streaming) mode.		
43	NGFW must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also. Vendor needs to add additional license if it is required.		
44	Antivirus module should be ICSA certified		
45	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.		
46	NGFW should have cloud sandbox functionality to protect organization from Advance Persistence Threats. In case any additional license is required, bidder has to include it in proposal from day one.		
47	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.		
48	NGFW should be able to monitor encrypted traffic to detect APTs hidden in SSL traffic.		
49	Buyer should get access of OEM's cloud portal from where he can view file-analysis status details including file submission time, source IP, destination IP, File name, URL, File size, File type, Suspicious Act etc.		
Web & DNS Security Functionalities			

50	The NGFW must have in-built Web Filtering Functionality		
51	The NGFW must have in-built Web Proxy functionality for HTTP and FTP protocols.		
52	The NGFW shall allow administrators to override Web Filtering database ratings with local settings		
53	The NGFW should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site's URL category thus blocking users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and sanctioned sites.		
54	NGFW should have 40000+ botnet definitions in its database and should be updated on regular basis to protect from new definitions		
55	The NGFW must have advanced URL filtering categories to block access to Newly Registered Domains, Newly Observed Domains, Dynamic DNS based websites.		
56	The NGFW must have capability to filter YouTube videos by using channel ID		
57	The NGFW must have option to rate web resource based on their DNS rating		
58	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware		
59	The NGFW must block Botnet C&C domains request at DNS level itself.		
60	The NGFW must have DNS Sinkhole functionality from day one to block and redirect malicious request to custom defined web portal.		
Data Leakage Prevention			
61	NGFW should have in-built DLP functionality without requiring any additional hardware or software license		
62	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.		
63	NGFW must detect, protect and log sensitive data travelling through protocols - HTTP, FTP, SMTP, IMAP, POP3, NNTP, MAPI, CIFS, SFTP, SCP		
64	DLP feature must offer watermarking functionality which allows organizers to apply document marking for DLP.		
65	DLP actions should be: Log only, block, quarantine user/IP/Interface		
66	It should have DLP fingerprinting feature which generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.		
High Availability			
67	The proposed NGFW shall have built-in high availability (HA) features without extra cost/license or hardware component		
68	The NGFW shall support stateful session maintenance in the event of a fail-over to a standby unit.		
69	High Availability feature must be supported for either NAT/Route, Transparent or Hybrid mode		
70	The NGFW must support both Active-Passive and Active-Active High Availability options.		
71	The NGFW must provide Load sharing mode along with redundancy in case multiple virtual firewalls are created on it.		
72	The NGFW shall support interface link monitoring failover		

73	The NGFW shall support external device ping probe failover		
74	The HA solutions should support silent firmware upgrade process that ensures minimum downtime		
75	The NGFW must have provision of fail-over in case of high memory utilisation on primary appliance.		
76	The NGFW must have capability to perform security inspection in networks where forward traffic and return traffic follow different paths.		
Administration, Management and Logging Functionality Feature Requirements			
77	Solution must offer separate appliance(s) either Physical or Virtual for centralized reporting to store logs and reports. In case of Virtual Appliance, necessary hardware & software will be provided by Organization Name.		

Technical Specification for 'DR INTERNAL FIREWALL-v1.2'

Sl. No.	Specification Minimum Required	Compliance Yes / No	Remarks
1.1	The proposed firewall vendor must be in Leader's quadrant of Gartner Enterprise Firewall report of 2021 for last three years		
1.2	The Firewall should be fixed Hardware based, Reliable, purpose-built security appliance with hardened operating system supporting State full policy inspection technology.		
Solution General Description			
2.1	The proposed solution shall have built-in high availability (HA) features without extra cost/license or hardware component		
2.2	The Solution must be supported both Active-Passive and Active-Active High Availability options		
2.3	The Solution must be deployed in Active-Active High Availability options.		
2.4	The Solution must be deployed in Full-Mesh		
2.5	The Solution must be supported and deployed in IPv4-IPv6 Dual Stack		
Firewall General Description			
3.1	Each Firewall appliance of the Solution must have 2 x GE RJ45 MGMT Ports, 2 x 10 GE SFP+ / GE SFP, HA Slots, 16 x GE RJ45 Ports, 8 x GE SFP Slots, 12 x 25 SFP28 / 10 GE SFP+/ GE SFP Slots, 4 x 100 GE QSFP28 / 40 GE QSFP+ Slots interfaces from day one. All these interfaces should be available simultaneously.		
3.2	Each Firewall appliance of the Solution must have minimum 4 x 100 Gbe Ethernet Ports along with 8 x 10G port & 16x1G ports from day-1 excluding Management and HA interface. Single Mode SFP (Fiber/Copper) for all ports needs to be provide as mentioned above		
3.3	Each Firewall appliance of the Solution must be rack mountable & have hot swappable dual power supply		
4	Each Firewall appliance of the Solution FW throughput should be at least 140 Gbps		
5	Each Firewall appliance of the Solution Threat Prevention (including FW, IPS, Application Control & Antivirus) throughput must be at least 15 Gbps with real-world / enterprise MIX traffic		
6	Each Firewall appliance of the Solution NGFW (including FW, IPS, Application Control) throughput must be at least 17 Gbps with real-world / enterprise MIX traffic		
7	Each Firewall appliance of the Solution NGFW should have IPsec VPN throughput of at least 55 Gbps		
8	Each Firewall appliance of the Solution NGFW should support 20000 site-to-site VPN Tunnels.		
9	Each Firewall appliance of the Solution NGFW should support more than 750000 new sessions per second		
10	Each Firewall appliance of the Solution should support at least 12 Million concurrent sessions		
11	The vendor must have a security gateway solution that can support the enablement of all next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus.		

12	Each Firewall appliance of the Solution should not introduce more than 3.22 microsecond latency. Vendor's claim must be available in publicly available documents like datasheet, admin guide etc. Claim on company's letterhead will not be acceptable.		
13	Each Firewall appliance of the Solution should support NAT64, NAT46, DNSv6 & DHCPv6		
14	The proposed system should be able to operate in Transparent (Access) mode and NAT/Route mode simultaneously without creating virtual context or virtual firewall		
15	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard, allowing the grouping of interfaces into a larger bandwidth 'trunk'. It should also allow for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk. NGFW should support ASIC based hardware,		
16	The NGFW should support WAN links load balancing and fail-over for at least 4 links		
17	The NGFW should support internet links load balancing and fail-over based parameters such as Latency, Jitter, Packet-Loss,		
18	The proposed system should have integrated Traffic Shaping functionality for both inbound and outbound traffic.		
19	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN) with minimum 10 Virtual Firewall license. And SD-WAN enabled from Day 1, all bandwidth cost should be provided from Day 1,		
20	The Firewall & IPSEC VPN module should have ICSA or other equivalent Certification.		
21	The NGFW should have both SSL and SSH Inspection capabilities		
22	The system should support 2 forms of site-to-site VPN configurations:		
23	a) Route based IPsec tunnel		
24	b) Policy based IPsec tunnel		
25	The system should support IPSEC site-to-site VPN and remote user IPSec VPN in transparent mode.		
26	The system should provide IPv6 IPsec feature to support for secure IPv6 traffic in an IPsec VPN.		
27	Solution must support at least 10 Gbps SSL-VPN Throughput		
28	The proposed firewall must support at least 10 Gbps of SSL Inspection throughput along with IPS feature enabled.		
29	Proposed NGFW must not require reboot to push security policies or any signature (IPS, Anti-malware etc.) update.		
30	The NGFW shall be able to support various form of user Authentication methods simultaneously, including: Local Database, LDAP, RADIUS, TACACS+, Windows AD, Citrix & Terminal Server Agent support for Single Sign On		
31	The NGFW should readily available integration with SDN platforms - Kubernetes, VMware ESXi and NSX, OpenStack, Cisco ACI, Nuage Networks and Nutanix		
Intrusion Prevention System			
31	Each Firewall appliance of the Solution IPS throughput should be at least 22 Gbps or better for Enterprise MIX traffic		
32	Each Firewall appliance of the Solution IPS should be able to inspect SSL sessions by decrypting the traffic		
33	Each Firewall appliance of the Solution IPS system should have at least		

	11,000 signatures		
34	In event if IPS should cease to function, it should fail open by default and be configurable so that crucial network traffic should not be blocked and NGFW should continue to operate while the IPS problem is being resolved		
35	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.		
36	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g., for severity level: high medium low)		
37	NGFW 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.		
Application Control Features:			
38	Each Firewall appliance of the Solution should have at least 4000 application signatures database		
39	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.		
40	Firewall must have capability to do Cloud application based routing not by means of manually adding IPs and or FQDNs i.e. firewall should have database of O365 readily available to select as destination address in firewall policy and destination address in static route configuration to give particular ISP path		
Anti-Malware & Advanced Persistent Threat			
41	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 and their equivalent encrypted versions, wherever applicable: HTTP, SMTP, POP3, IMAP, FTP, CIFS, NNTP, SSH, MAPI		
42	NGFW should offer both anti-virus scanning options - Proxy mode and Flow (streaming) mode.		
43	NGFW must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also. Vendor needs to add additional license if it is required.		
44	Antivirus module should be ICSA certified		
45	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.		
46	NGFW should have cloud sandbox functionality to protect organization from Advance Persistence Threats. In case any additional license is required, bidder has to include it in proposal from day one.		
47	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.		
48	NGFW should be able to monitor encrypted traffic to detect APTs hidden in SSL traffic.		
49	Buyer should get access of OEM's cloud portal from where he can view file-analysis status details including file submission time, source IP, destination IP, File name, URL, File size, File type, Suspicious Act etc.		

Web & DNS Security Functionalities			
50	The NGFW must have in-built Web Filtering Functionality		
51	The NGFW must have in-built Web Proxy functionality for HTTP and FTP protocols.		
52	The NGFW shall allow administrators to override Web Filtering database ratings with local settings		
53	The NGFW should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site's URL category thus blocking users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and sanctioned sites.		
54	NGFW should have 40000+ botnet definitions in its database and should be updated on regular basis to protect from new definitions		
55	The NGFW must have advanced URL filtering categories to block access to Newly Registered Domains, Newly Observed Domains, Dynamic DNS based websites.		
56	The NGFW must have capability to filter Youtube videos by using channel ID		
57	The NGFW must have option to rate web resource based on their DNS rating		
58	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware		
59	The NGFW must block Botnet C&C domains request at DNS level itself.		
60	The NGFW must have DNS Sinkhole functionality from day one to block and redirect malicious request to custom defined web portal.		
Data Leakage Prevention			
61	NGFW should have in-built DLP functionality without requiring any additional hardware or software license		
62	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.		
63	NGFW must detect, protect, and log sensitive data travelling through protocols - HTTP, FTP, SMTP, IMAP, POP3, NNTP, MAPI, CIFS, SFTP, SCP		
64	DLP feature must offer watermarking functionality which allows organizers to apply document marking for DLP.		
65	DLP actions should be: Log only, block, quarantine user/IP/Interface		
66	It should have DLP fingerprinting feature which generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.		
High Availability			
67	The proposed NGFW shall have built-in high availability (HA) features without extra cost/license or hardware component		
68	The NGFW shall support stateful session maintenance in the event of a fail-over to a standby unit.		
69	High Availability feature must be supported for either NAT/Route, Transparent or Hybrid mode		
70	The NGFW must support both Active-Passive and Active-Active High Availability options.		
71	The NGFW must provide Load sharing mode along with redundancy in case multiple virtual firewalls are created on it.		
72	The NGFW shall support interface link monitoring failover		

73	The NGFW shall support external device ping probe failover		
74	The HA solutions should support silent firmware upgrade process that ensures minimum downtime		
75	The NGFW must have provision of fail-over in case of high memory utilisation on primary appliance.		
76	The NGFW must have capability to perform security inspection in networks where forward traffic and return traffic follow different paths.		
Administration, Management and Logging Functionality Feature Requirements			
77	Solution must offer separate appliance(s) either Physical or Virtual for centralized reporting to store logs and reports. In case of Virtual Appliance, necessary hardware & software will be provided by Organization Name.		

Technical Specification for 'DR Perimeter Firewall-v1.0'

Sr. no	Specification Minimum Required	Compliance Yes / No	Remarks
1	Each appliance of the Solution must be a purpose built chassis or hyperscale solution to deliver minimum 100 Gbps of NGFW throughput including firewall, application control & intrusion prevention (ips) features enabled from day 1 & scalable up to 250 Gbps in future. Each appliance of the Solution should support 100 Gbps IPS throughput from day 1 & scalable upto 250Gbps in future. The architecture should support on-demand scaling of throughput to accommodate future growth & expansion		
Solution General Description			
2.1	The proposed solution shall have built-in high availability (HA) features without extra cost/license or hardware component		
2.2	The Solution must be supported both Active-Passive and Active-Active High Availability options		
2.3	The Solution must be deployed in Active-Active High Availability options.		
2.4	The Solution must be deployed in Full-Mesh		
2.5	The Solution must be supported and deployed in IPv4-IPv6 Dual Stack		
Firewall General Description			
3	Each appliance of the Solution must have minimum 6 x 25 GbE Fibre Ports along with 6 x 100G ports from day-1. Each appliance of the Solution device must have interface scalability for 4X 100G ports in future within the same appliance. All transceivers must be provided by the bidder. All SFR should be SR		
4	Each appliance of the Solution should facilitate to apply unified threat policy like AV, IPS policy for ease of use.		
5	Each appliance of the Solution must be rack mountable. Mounting kit must be provided by the bidder.		
6	Integrated IPS must have 4000+ signature database including the SCADA and other industrial threats. It should support creation of custom IPS signature and creation of multiple IPS policy for different zone		
7	Each appliance of the Solution must have hot swappable dual power supply		
8	The Solution should support maximum concurrent sessions up to minimum 20 Million and support minimum 400K New Sessions/sec		
9	Each appliance of the Solution should have minimum 128 GB RAM		
10	vendor must be Leaders in Gartner magic quadrant for Enterprise Each appliance of the Solution for minimum 3 years		
11	The vendor must have a security gateway solution that can support the enablement of all next generation Each appliance of the Solution security applications, including intrusion protection, application control, URL filtering, threat prevention (like anti-bot, anti-virus), sandboxing all managed from a central platform.		
12	Solution must block threats/malware/unknown attacks in real-time & should not allow any zero-day threat in network by proactively removing any possibility of malicious content.		
13	Solution must support gateway high availability in active-active mode.		
14	IPS must support network exceptions based on source, destination, service, or a combination of the three		
15	Must be able to acquire user identity by querying Microsoft Active Directory based on security events		

16	The solution must provide a mechanism to limit application usage based on bandwidth consumption		
17	The solution should have detection and prevention capabilities for DNS tunnelling attacks		
18	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other		
19	The Log Viewer should have the ability view all of the security logs (fw,IPS ,urlf...) in one view pane (helpful when troubleshooting connectivity problem for one IP address)		
20	Each appliance of the Solution must be field upgradable as per architecture for additional ports/transceivers.		
21	Each appliance of the Solution solution Must allow security rules to be enforced within time intervals to be configured with an expiry date/time.		
22	The management must provide a security rule hit counter in the security policy		
23	Solution must include predefined hourly, daily, weekly, and monthly reports. Including at least Top events, Top sources, Top destinations, Top services, Top sources and their top events, Top destinations and their top events and Top services and their top events		
24	Solution must include preconfigured graphs to monitor the evolution in time of traffic and system counters. Solution must provide the option to generate new customized graphs with different chart types		
25	Solution must include customizable threshold setting to take actions when a certain threshold is reached on a gateway. Actions must include Log, alert, send an SNMP trap, send an email and execute a user defined alert		
26	Vendor must provide details on the re-categorization of URL, under the circumstances that a website has been comprised and possibly distributing malware		
27	The communication between the management servers and the security gateways must be encrypted and authenticated with PKI Certificates.		
28	It should be able to protect against Denial of Service (DOS) attacks and able to block unwanted traffic of P2P file sharing, IM traffic if required		
29	Solution GUI must provide a comprehensive search across all policies.		
30	The central logging must be part of the hardware-based management system. Alternatively, administrators must have ability to install dedicated Log Servers in case needed in future		
31	The Each appliance of the Solution should have detection and prevention capabilities for C&C DNS hideouts: Reverse engineer malware in order to uncover their DGA (Domain Name Generation)		
32	The Solution should offer support for SSL Inspection/Decryption considering futuristic if needed on the device		
33	The manufacturer should have Technical Assistance Centre (TAC) based in India.		
34	The Each appliance of the Solution should have remote VPN solution to cater to 200 remote VPN concurrent users.		
35	Solution must include a local user database to allow user authentication and authorization without the need for an external device		
36	IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behaviour-based detection		
37	IPS must provide at least two pre-defined profiles/policies that can be used immediately		
38	IPS application must have a centralized event correlation and reporting mechanism		
39	IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP, Windows services (Microsoft Networking)		
40	Solution must provide different logs for regular user activity and management related logs		
41	Solution must include a tool to correlate events from all the gateway features and devices		

42	Each appliance of the Solution should not be an ASIC based Each appliance of the Solution & should be based on multi-core CPU architecture		
43	The solution should support linear scalability in future as on when required. The solution should be able to support N+1 Redundancy from day-1. The solution should not be dependent for any 3rd party hardware/software to achieve redundancy.		
44	Each appliance of the Solution should support following threat prevention features like antivirus, anti-malware, anti-bot, dns security, url-filtering, zero-phishing		
Management			
45	The management must be centralised and should be in a hardware form. It should support High Availability		
46	The solution shall provide a single console to manage all the firewalls and provide visibility across the infrastructure		
47	The solution shall allow creation of objects and policies at a central place and allow it to be deployed to the managed devices.		
48	The solution shall allow detailed revision tracking of policies and have auditing mechanism to track changes.		
49	The solution shall allow configuration backup of the managed devices.		
50	The solution shall provide centralized software upgrades and security updates for the managed devices		
51	The solution shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges.		
52	Security management must provide set of built-in security best practices which provide automatic score for various security regulations		

Technical Specification for 'DR Perimeter Firewall-v1.1'

Sr. no	Specification Minimum Required	Compliance Yes / No	Remarks
1	The proposed firewall vendor must be in Leader's quadrant of Gartner Enterprise Firewall report for last 3 years		
2	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system supporting State full policy inspection technology.		
3	Firewall appliance must have 4x40 GE QSFP+ Slots populated with multimode transceiver, 10 x 10GE SFP+/SFP 28 slots populated with multimode transceiver, 8 x 1GE SFP slots populated with multimode transceiver & 10 x 1GE RJ45 interfaces from day one. All these interfaces should be available simultaneously from day one.		
4	Firewall Throughput should be at least 85 Gbps		
6	NGFW (including FW, IPS, Application Control) throughput must be at least 15 Gbps with real-world / enterprise MIX traffic		
7	NGFW should have IPsec VPN throughput of at least 40 Gbps		
8	NGFW should support more than 500 site-to-site VPN Tunnels.		
9	NGFW should support more than 500,000 new sessions per second		
10	NGFW should support at least 10 Million concurrent sessions		
11	NGFW should not introduce more than 10 microsecond latency. Vendor's claim must be available in publicly available documents like datasheet, admin guide etc. Claim on company's letterhead will not be acceptable.		
12	The NGFW solution should support NAT64, NAT46, DNSv6 & DHCPv6		
13	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard, allowing the grouping of interfaces into a larger bandwidth 'trunk'. It should also allow for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk.		
14	The NGFW should support WAN links load balancing and fail-over for at least 4 links		
15	The NGFW should support internet links load balancing and fail-over based parameters such as Latency, Jitter, Packet-Loss,		
16	The proposed system should have integrated Traffic Shaping functionality for both inbound and outbound traffic.		
17	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN) with minimum 4 Virtual Firewall license.		
18	The Firewall & IPSEC VPN module should have ICSA or other equivalent Certification.		
19	The NGFW should have both SSL and SSH Inspection capabilities		
20	The system should support 2 forms of site-to-site VPN configurations:		
20.1	a) Route based IPsec tunnel: Multiple ISP active route-based tunnel in full mesh. BGP v4, OSPF v2 and v3 must support over route-based IPsec site to site tunnel. It must support third party firewalls and routers.		
20.2	b) Policy based IPsec tunnel		
21	The system should support IPSEC site-to-site VPN and remote user IPsec VPN in transparent mode.		

22	The system should provide IPv6 IPsec feature to support for secure IPv6 traffic in an IPsec VPN.		
23	The firewall should support custom IPS signatures		
24	The proposed firewall must support at least 10 Gbps of SSL Inspection throughput along with IPS feature enabled.		
25	Proposed NGFW must not require reboot to push security policies or any signature (IPS, Anti-malware etc.) update.		
26	The NGFW shall be able to support various form of user Authentication methods simultaneously, including Local Database, LDAP, RADIUS, TACACS+, Windows AD, Citrix & Terminal Server Agent support for Single Sign On		
27	The NGFW should readily available integration with SDN platforms - Kubernetes, VMware ESXi and NSX, OpenStack, Cisco ACI, Nuage Networks and Nutanix		
	Intrusion Prevention System		
28	IPS throughput should be at least 15 Gbps or better for Enterprise MIX traffic		
29	The IPS should be able to inspect SSL sessions by decrypting the traffic		
30	The IPS system should have at least 6,000 signatures		
31	In event if IPS should cease to function, it should fail open by default and be configurable so that crucial network traffic should not be blocked and NGFW should continue to operate while the IPS problem is being resolved		
32	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 lookups.		
33	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)		
34	NGFW 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.		
	Application Control Features:		
36	The appliance should have at least 4000 application signatures database		
37	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.		
38	Firewall must have capability to do Cloud application-based routing not by means of manually adding IPs and or FQDNs i.e. firewall should have database of O365 readily available to select as destination address in firewall policy and destination address in static route configuration to give particular ISP path		
	Anti-Malware & Advanced Persistent Threat		
39	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 and their equivalent encrypted versions, wherever applicable: HTTP, SMTP, POP3, IMAP, FTP, CIFS, NNTP, SSH, MAPI		
40	NGFW should offer both anti-virus scanning options - Proxy mode and Flow (streaming) mode.		
41	NGFW must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also. Vendor needs to add additional license if it is required.		

42	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.		
43	NGFW should have cloud sandbox functionality to protect organization from Advance Persistence Threats. In case any additional license is required, bidder has to include it in proposal from day one.		
44	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.		
45	NGFW should be able to monitor encrypted traffic to detect APTs hidden in SSL traffic.		
46	Buyer should get access of OEM's cloud portal from where he can view file-analysis status details including file submission time, source IP, destination IP, File name, URL, File size, File type, Suspicious Act etc.		
	Web & DNS Security Functionalities		
47	The NGFW must have in-built Web Filtering Functionality		
48	The NGFW must have in-built Web Proxy functionality for HTTP and FTP protocols.		
49	The NGFW shall allow administrators to override Web Filtering database ratings with local settings		
50	The NGFW should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site’s URL category thus blocking users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and sanctioned sites.		
51	The NGFW must have advanced URL filtering categories to block access to Newly Registered Domains, Newly Observed Domains, Dynamic DNS based websites.		
52	The NGFW must have capability to filter Youtube videos by using channel ID		
53	The NGFW must have option to rate web resource based on their DNS rating		
54	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware		
55	The NGFW must block Botnet C&C domains request at DNS level itself.		
56	The NGFW must have DNS Sinkhole functionality from day one to block and redirect malicious request to custom defined web portal.		
	Data Leakage Prevention		
57	NGFW should have in-built DLP functionality without requiring any additional hardware or software license		
58	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.		
59	NGFW must detect, protect and log sensitive data travelling through protocols - HTTP, FTP, SMTP, IMAP, POP3, NNTP, MAPI, CIFS, SFTP, SCP		
60	DLP feature must offer watermarking functionality which allows organizers to apply document marking for DLP.		
61	DLP actions should be : Log only, block, quarantine user/IP/Interface		
62	It should have DLP fingerprinting feature which generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint		

	database.		
	High Availability		
63	The proposed NGFW shall have built-in high availability (HA) features without extra cost/license or hardware component		
64	The NGFW shall support stateful session maintenance in the event of a fail-over to a standby unit.		
65	High Availability feature must be supported for either NAT/Route, Transparent or Hybrid mode		
66	The NGFW must support both Active-Passive and Active-Active High Availability options.		
67	The NGFW must provide Load sharing mode along with redundancy in case multiple virtual firewalls are created on it.		
68	The NGFW shall support interface link monitoring failover		
69	The NGFW shall support external device ping probe failover		
70	The HA solutions should support silent firmware upgrade process that ensures minimum downtime		
71	The NGFW must have provision of fail-over in case of high memory utilisation on primary appliance.		
72	The NGFW must have capability to perform security inspection in networks where forward traffic and return traffic follow different paths.		
	Administration, Management and Logging Functionality Feature Requirements		
73	Solution must offer separate appliance(s) either Physical or Virtual for centralized reporting to store logs and reports. In case of Virtual Appliance, necessary compute and storage will be provided by TP ODISHA DISCOMS. Bidder needs to mention the system requirement for the same. All the needed connectivity and integration will be at the Bidder scope. Due diligence is recommended.		
74	Separate reporting appliance must offer at least 900Gb internal storage space. (Clause is applicable for physical appliance only)		
75	Centralized reporting solution must be capable to accept 40GB of logs per day from day one and option should be capable to increase 80 GB logs per day by additional license in future if require (additional license need to purchase separately).		
76	Logs should also show real-time per user statistics which must include sent/receive bytes, no. of sessions, threat score, bandwidth usage, sent/receive packets & source IP or user, destination country detail		
77	Logging and reporting solution must have ready-made report template such as Top Users, Top Application, Top Destinations, Interface utilization per device per link, CPU and Memory usage of each device, malware / threat analysis report etc.		
78	Logging and reporting appliance should also send an alert in case of WAN link failure and recovery		
79	Traffic reports: availability, bandwidth usage per access circuit, bandwidth usage per application, latency, packet loss, QoS per access circuit etc.		
80	It should support retrieving of archived logs to perform analytics against		

	historic data		
81	Reporting solution should provide detailed Event analysis for Firewall and IPS and also should provide Syslog output to integrate with other major SIEM tools		
82	The solution should provide flexible report formats like HTML/CSV/XML/PDF		
	Warranty & Support		
83	The proposed solution should be offered with 5 years of support from day one.		
83	The proposed solution should be offered with 5 years of support from day one.		
	Sandboxing Appliance		
84	The solution should support deep packet inspection of SSL encrypted traffic (including HTTPS) for both incoming and outgoing		
85	The solution should provide detection, analysis and remediation capability against APT & SSL based APT attacks.		
86	The solution must employ an on premise (not on cloud) analysis engine using virtual execution to detect zero day and unknown threats and must not be signature based.		
87	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.		
88	The proposed solution should perform dynamic real-time analysis of advanced malware to confirm true zero-day and targeted attacks. No file should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware		
89	The proposed solution should automatically detect and confirm multistage zero day malware and targeted attacks without prior knowledge of the malware.		
90	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.		
91	The proposed solution should analyse advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications.		
92	The solution must support pre-populated Licensed copies of Operating systems and applications/softwares (like Microsoft Office). There should be no requirement for the customer to buy additional license.		
93	The system should be able to support file sizes upto 50 mb or more		
94	The proposed solution should have the ability to analyse, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents,		
95	common multimedia contents such as JPEG/GIF/BMP/WMF and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zero-day attacks.		
96	The proposed solution should capture, and store packet captures of traffic relevant to the analysis of detected threats.		
97	The proposed solution should have the ability to display the geo-location of the remote command and control server(s) when possible.		
98	The proposed solution should have the ability to report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack.		

99	The proposed solution should be able to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, or SNMP).		
100	The proposed solution should have the ability to be deployed in out-of-band mode (also SPAN/TAP) & inline mode		
101	The proposed solution should be capable to block inbound malicious exploits delivered via a web channel and outbound call-back communications when deployed in inline, or out-of-band mode.		
102	The proposed solution should be able to analyse email attachments and malicious links for static and dynamic analysis		
103	The proposed solution should support SMB / CIFS / NFS protocol for sharing and transferring files		
104	The proposed solution should provide visibility into scan histories of each file scanned that are aborted, completed, or in progress.		
105	The solution should provide reports in (but not limited to) PDF/CSV formats.		
106	The solution should have anti-evasion capabilities to prevent malwares detection of being run/executed in the virtualized environment.		
107	The proposed solution should have capability to analyse saved email (.eml) files for malicious attachments.		
108	The solution should protect the endpoints against advanced threats including zero-day attacks, which target application vulnerabilities that have yet to be discovered or patched.		
109	The solution should protect the endpoint by monitoring the host memory to detect and block various memory techniques like return-oriented programming, heap spraying, etc.		
110	The endpoint solution should be able to prevent attacks from known and unknown malwares		
111	The endpoint solution should protect against drive-by download attacks and provide shield to web browsers, Java/Flash plug-ins, Microsoft Office applications, and PDF readers		
112	The solution should support for SIEM log integration.		
113	The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc.		
114	Minimum number of Interfaces - 4x GE & 2 x 10G		
115	Number of VM's should be at least 24		
116	It should support Sandbox Analysis for multiple operating systems like WinXP, Win7, Win8, Win10		
117	The APT appliance should be able to process minimum of 450 files/hour or 3,00,000 files/month (either web or mail or both) on the VM sandboxing		
118	High Availability & Maximum Scalability		
119	The solution should have dual AC power supply fully populated (within box) from day one		

Technical Specification for 'Sandbox'

Sr. no	Specification Minimum Required	Compliance Yes / No	Remarks
1	The sandboxing appliance should have at least 24 VM instances internally and should emulate at least 2200 unique/real world files per hour		
2	The sandboxing solution should be able to inspect, emulate, prevent and share the results of the sandboxing event into the anti-malware infrastructure		
3	The sandboxing appliance should support a minimum throughput of 2 Gbps along with support for both 1G and 10G Interfaces		
4	Solution’s reaction time to a potential threat should be no longer than 5 Mins.		
5	The solution must be able to clean/remove the following active content types: Database queries Embedded objects Fast save data Linked objects Macros and code PDF GotoR actions PDF launch actions PDF URI actions PDS sound actions PDF movie actions PDS JavaScript Actions PDF Submit Form actions Sensitive hyperlinks		
6	The solution must have the following anti evasion technic technologies implemented: • VM detection • time delays • shut-down, re-start VM detection • user interaction		
7	The sandbox must have the capability to open password protected ZIP files		
8	The solution must provide the ability to Protect against zero-day & unknown malware attacks before static signature protections have been created		

9	The solution should support Network based sandboxing		
10	Sandboxing engine should detect API calls, file system changes, system registry, network connections, system processes.		
11	The solution must be able to sandbox different sizes of files for sandboxing, with file sized up to 100Mb		
12	The sandbox execution must support on premise mode		
13	The solution must detect the attack at the exploitation stage – i.e., before the shell-code is executed and before the malware is downloaded / executed.		
14	supports archive type files: Zip, Cab,7z, rar, tgz, tar		
15	The sandboxing solution to prevent from unknown attacks in real-time should be a hardware device deployed in Tata Power's DC		

	Scope of Work & Service Level Agreement		
Sl. No.	**Description**	**Compliance**	**Remarks**
1	**Terms of Agreement:**		
	This agreement shall remain in force from the date of commencement i.e., <date > till the expiry of the warranty (including extension if any) for the device provided against this order. It shall be open to TP Odisha discoms to terminate this agreement any time during its currency by giving one month notice to the vendor, in writing.		
	Perimeter Firewall and Sandbox solution should be from same OEM.		
	Internal Firewall and Perimeter Firewall solution should be from different OEM.		
2	**Commencement of Warranty Period**		
	The warranty/support period will start from date of completion of installation of device i.e., from the date on which installation report is signed by TP Odisha discoms		
	a) The warranty of the equipment's carries for 5 years warranty. Vendor shall provide maintenance of the equipment's for a period 5 years as per terms and laid in this document. Conditions laid in this document.		
	b) Vendor shall be authorized channel partner of OEM. Vendor shall submit the authorization certificate (MAF) form OEM along with this SLA.		
	c) Uptime guarantee: Uptime of the equipment's will be 99 %. This will be calculated on monthly basis.		
3	**Scope of Work**		
	TP Odisha discoms nominated person release RO/mail for Installation of appliance/software at TP Odisha discoms area. (Scope of Installation area will be across TP Odisha discoms DC/DRC)		
	a) Studying existing physical and virtual IT infra / network setup in consultant with TP Odisha discoms IT team. (Including Network Security, MPLS, SAN, Spine leaf architecture, Server and IPv6, etc)		
	b) OEM should prepare/certified landscape/diagram/HLD/LLD		
	c) Mounting of the appliance in the rack.		
	d) Installing the related hardware/software components and terminating the cables on network devices.		
	e) Complete configuration of the device to integrate with existing DC and DRC network.		
	f) Implement and documentation of the same		
	g) Test all the services.		
	h) Provide Hands on Training to TP Odisha discoms Team (Minimum 12 Engineer) by OEM only.		
	i) Vendor should complete the project as per the agreed time.		
	j) OEM Team/Engineer should do the implementation services at site (TPSODL/TPCODL/TPWODL/TPNODL)		
	K) Supply and installation of necessary cables, accessories (Power cord for Indian standard, cable tie etc.) (Optical patch card/Cat6) & SFP for		

	interconnecting to Firewall/Router/Servers/Leaf switches/Management switches with sufficient quantity. Quantity will be decided at the time of Implementations.		
4	**Maintenance Services**		
	Vendor shall provide maintenance services under this agreement for the equipment listed above on per agreed vide purchase order number for the purchased equipment.		
	The maintenance services shall include the following: -		
	(i) Corrective Maintenance		
	Any system failure, service will be attended by vendor's engineer and if necessary, by their specialists and consultant. If any spare parts or full system requires replacement, it should be replaced with equivalent model or higher model only. Till the time spare part / services is replaced/restored, entire appliance will be considered to be down.		
	(ii) Preventive Maintenance		
	TP Odisha discoms will allow vendor to carry out required Preventive Maintenance of the device. The down time required for Preventive Maintenance will be included in total down time of system to calculate quarterly uptime and also communicated to TP Odisha discoms management by the vendor.		
5	**Spares Availability/ Support for OS Patch**		
	Vendor shall have a back-to-back Business Critical Support arrangement with the <OEM> for spares and escalation support. Vendor shall also have a formal arrangement with < OEM> for any technical support that may be required on the hardware and the OS.		
	A copy of agreement between service provider & OEM should be provided to TP Odisha discoms		
	The deliveries under system Hardware, software/patches support include: -		
	System Software (IOS) updates / upgrades		
	Pro-active patch notification & installation on device		
	Operating System Bug-fixes		
	Flash memory up gradation		
	Access to OEM Diagnostic Solutions Database.		
	Any other changes beneficial to TP Odisha discoms will be done on device through the bidder		
6	**Response and Resolution Time**		
	As mentioned in SLA		
7	**Delivery Time**		
	The devices should be delivered within 6-8 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (Client will intimate date to bidder for installation of equipment's).		
8	**Method of contact to Engineer**		
	Vendor should mention contact no, e-mail id and name of concerned Engineer		
9	**Level of specialist assistance to engineer.**		

	The vendor will ensure that all required specialist /Technical Support will be provided to his engineer so that the guaranteed uptime will be achieved		
	Level of Escalation (If problem is not resolved as per SLA)		
	Level 1 – The Account Manager <Ph number, Email id>		
	Level 2 – General Manager or Equivalent Level <Ph number, Email id>		
	Level 3 – CEO of the company <Ph number, Email id>		
10	**Reporting**		
	The vendor shall prepare a Monthly Report in the prescribed format of TP Odisha discoms covering the following - Uptime Summary Report		
11	**Liquidated Damages**		
	In case uptime commitment of device (as mentioned in clause 2 (a), (c), 3, 5, 6, 7, 8)) of this SLA) is not met, the same would attract a Penalty @ Rs1000 per hour per device. The penalty money will be recovered from the payment due to vendor.		

Service Level Agreement (SLA)

Sl. No	Activity	SLA Timelines
1	Configuration/ Call Response Time	2 Hours response time.
2	Resolution Time	4 hours from the time of call registration.
3	Spares/Hardware Failure	NBD or Replacement as per the OEM support terms

Escalation Matrix:

Category	On call Response	Contact person	Email id
Support – Initial analysis (L1)	Within 4hrs		
L2	Within 6Hrs		
Account Manager			
Sales Director			

TPCODL TPNODL TPSODL TPWODL

TP Central Odisha Distribution Limited TP Northern Odisha Distribution Limited TP Southern Odisha Distribution Limited TP Western Odisha Distribution Limited

CENTRALIZED CONTRACTS GROUP

For Reference- User Manual e-Bidding & Auction (Ariba)

SUPPLIER MANUAL ANSWERING TO E-BIDDING

	Version 1.2
Company Confidential	DEC - 2020

INDEX

1 ACCESSING ARIBA SOURCING **3**

2 VENDOR SCREEN **4**

2.1.1 Review and Approve "Prerequisites" *5*

2.1.2 Select Items or Lots *6*

2.1.3 Entering Your Prebid *6*

2.1.4.1 How to submit a price 9

3 COMMUNICATING WITH TATA POWER BUYER DURING E-BIDDING **7**

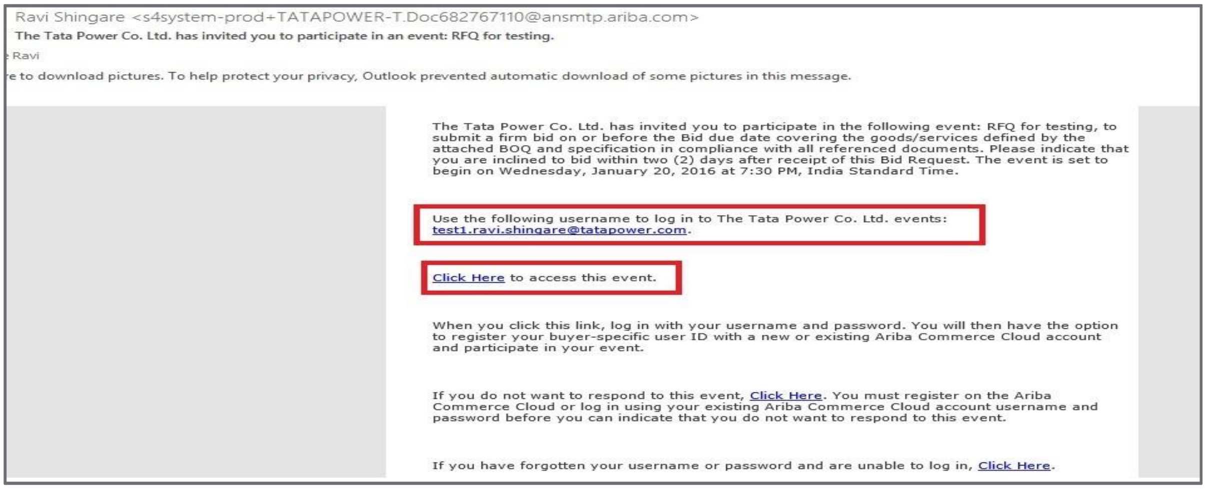
4 ARIBA TRAINING AND ARIBA SUPPORT **8**

5 SUPPLIER FREQUENTLY ASKED QUESTION **11**

1- Accessing Ariba Sourcing

Step 1: You will get an invitation to your email from Ariba System. Keep this email, it contains your login Information and a direct link to Ariba.

Step 2: Click “Click Here” to access the Ariba Web Site.



Ravi Shingare <s4system-prod+TATAPOWER-T.Doc682767110@ansmtp.ariba.com>

The Tata Power Co. Ltd. has invited you to participate in an event: RFQ for testing.

Ravi

e to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

The Tata Power Co. Ltd. has invited you to participate in the following event: RFQ for testing, to submit a firm bid on or before the Bid due date covering the goods/services defined by the attached BOQ and specification in compliance with all referenced documents. Please indicate that you are inclined to bid within two (2) days after receipt of this Bid Request. The event is set to begin on Wednesday, January 20, 2016 at 7:30 PM, India Standard Time.

Use the following username to log in to The Tata Power Co. Ltd. events: test1.ravi.shingare@tatapower.com.

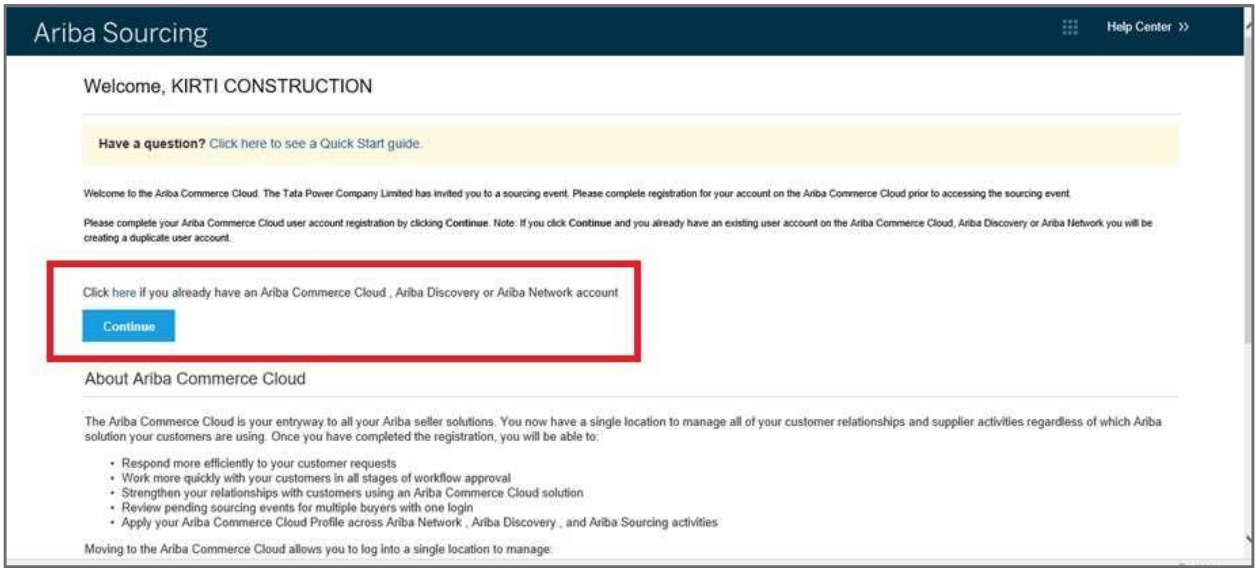
Click Here to access this event.

When you click this link, log in with your username and password. You will then have the option to register your buyer-specific user ID with a new or existing Ariba Commerce Cloud account and participate in your event.

If you do not want to respond to this event, Click Here. You must register on the Ariba Commerce Cloud or log in using your existing Ariba Commerce Cloud account username and password before you can indicate that you do not want to respond to this event.

If you have forgotten your username or password and are unable to log in, Click Here.

Step 3: Supplier has to click on "Continue"



Welcome, KIRTI CONSTRUCTION

Have a question? Click here to see a Quick Start guide.

Welcome to the Ariba Commerce Cloud. The Tata Power Company Limited has invited you to a sourcing event. Please complete registration for your account on the Ariba Commerce Cloud prior to accessing the sourcing event.

Please complete your Ariba Commerce Cloud user account registration by clicking **Continue**. Note: If you click **Continue** and you already have an existing user account on the Ariba Commerce Cloud, Ariba Discovery or Ariba Network you will be creating a duplicate user account.

Click here if you already have an Ariba Commerce Cloud , Ariba Discovery or Ariba Network account

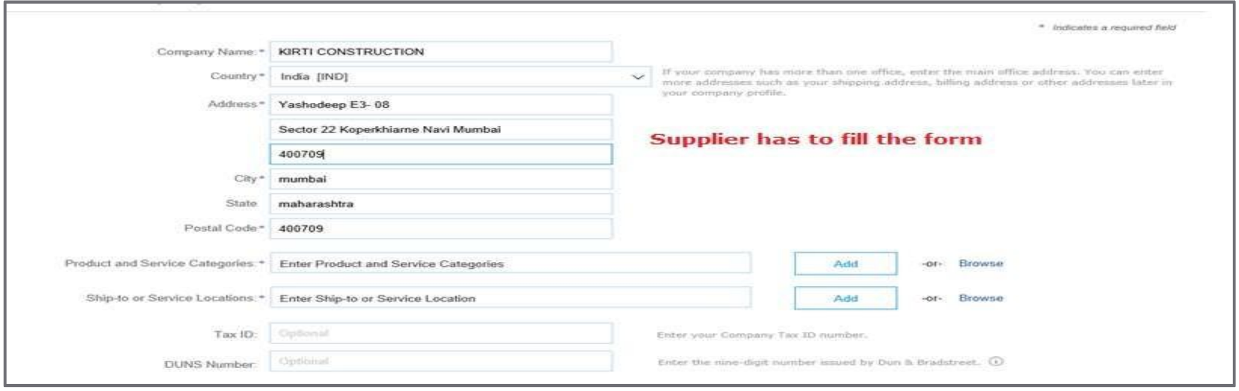
About Ariba Commerce Cloud

The Ariba Commerce Cloud is your entryway to all your Ariba seller solutions. You now have a single location to manage all of your customer relationships and supplier activities regardless of which Ariba solution your customers are using. Once you have completed the registration, you will be able to:

- Respond more efficiently to your customer requests
- Work more quickly with your customers in all stages of workflow approval
- Strengthen your relationships with customers using an Ariba Commerce Cloud solution
- Review pending sourcing events for multiple buyers with one login
- Apply your Ariba Commerce Cloud Profile across Ariba Network , Ariba Discovery , and Ariba Sourcing activities

Moving to the Ariba Commerce Cloud allows you to log into a single location to manage:

Step 4: The registration process only takes a few moments, with a simple one-page registration Define your password and secret question. Click “OK”



* Indicates a required field

Company Name: * KIRTI CONSTRUCTION

Country * India [IND]

If your company has more than one office, enter the main office address. You can enter more addresses such as your shipping address, billing address or other addresses later in your company profile.

Address * Yashodeep E3- 08
Sector 22 Koperkhiarne Navi Mumbai
400709

City * mumbai

State maharashtra

Postal Code * 400709

Product and Service Categories: * Enter Product and Service Categories

Ship-to or Service Locations: * Enter Ship-to or Service Location

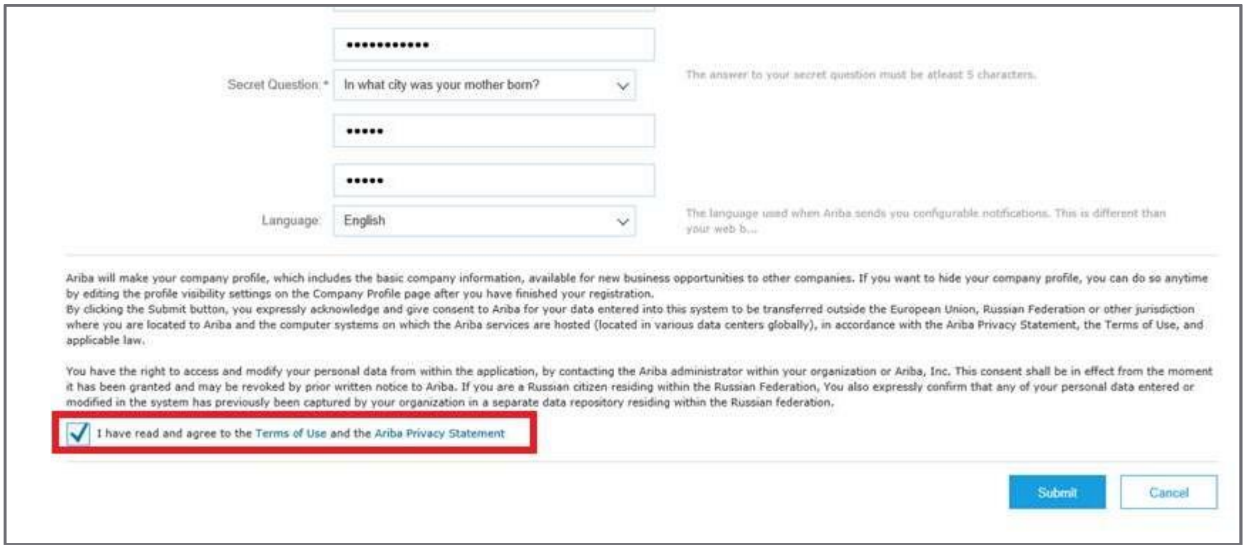
Tax ID: Optional

Enter your Company Tax ID number.

DUNS Number: Optional

Enter the nine-digit number issued by Dun & Bradstreet.

Step 5: If it’s the first time you are invited to use UPM Ariba, you’ll need to accept the “Participant Terms”. Select “I accept the terms of this agreement”. Click “Submit”.



••••••••••••

Secret Question: * In what city was your mother born?

The answer to your secret question must be atleast 5 characters.

•••••

•••••

Language: English

The language used when Ariba sends you configurable notifications. This is different than your web b...

Ariba will make your company profile, which includes the basic company information, available for new business opportunities to other companies. If you want to hide your company profile, you can do so anytime by editing the profile visibility settings on the Company Profile page after you have finished your registration.
By clicking the Submit button, you expressly acknowledge and give consent to Ariba for your data entered into this system to be transferred outside the European Union, Russian Federation or other jurisdiction where you are located to Ariba and the computer systems on which the Ariba services are hosted (located in various data centers globally), in accordance with the Ariba Privacy Statement, the Terms of Use, and applicable law.

You have the right to access and modify your personal data from within the application, by contacting the Ariba administrator within your organization or Ariba, Inc. This consent shall be in effect from the moment it has been granted and may be revoked by prior written notice to Ariba. If you are a Russian citizen residing within the Russian Federation, You also expressly confirm that any of your personal data entered or modified in the system has previously been captured by your organization in a separate data repository residing within the Russian federation.

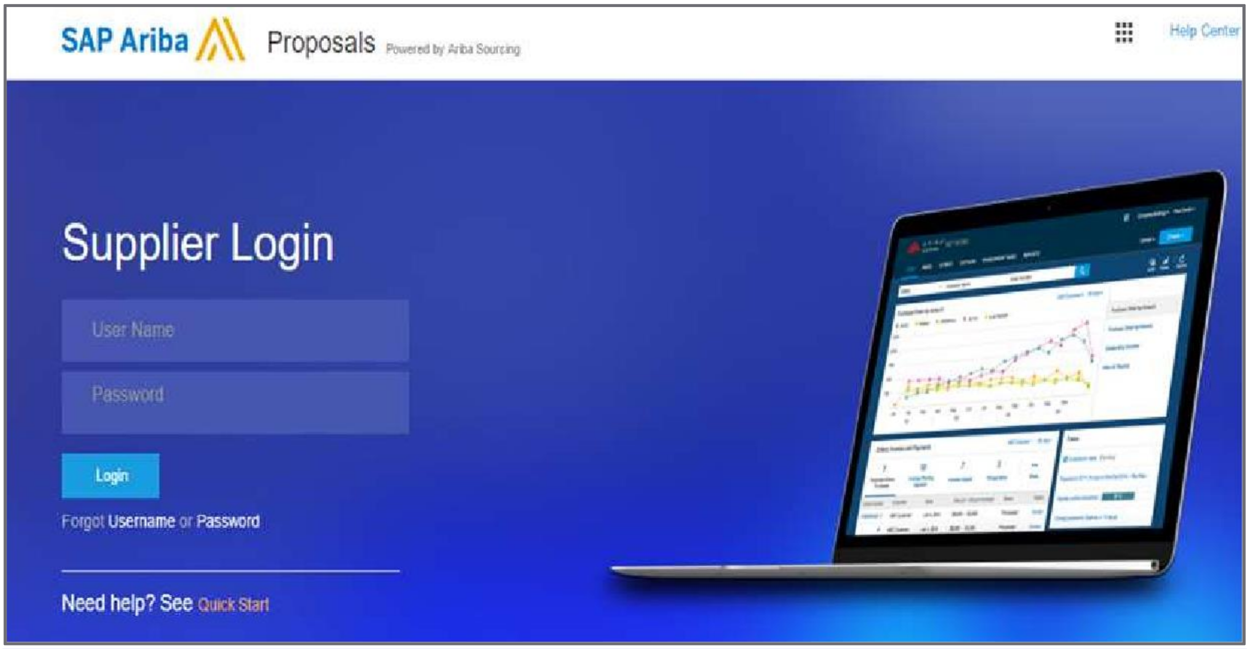
☑ I have read and agree to the Terms of Use and the Ariba Privacy Statement

2 Vendor Screen - Submitting Your Answers / Proposal

2.1.1 If vendor goes through mail invitation then directly Screen 3.1.1 will appear, but if If you have used Ariba before and have already accessed an event for the buyer-specific account with your current log in ID, click the **Login** button to continue. Log in with your Ariba username and password in order to participate in the event OR you have to follow the following steps.

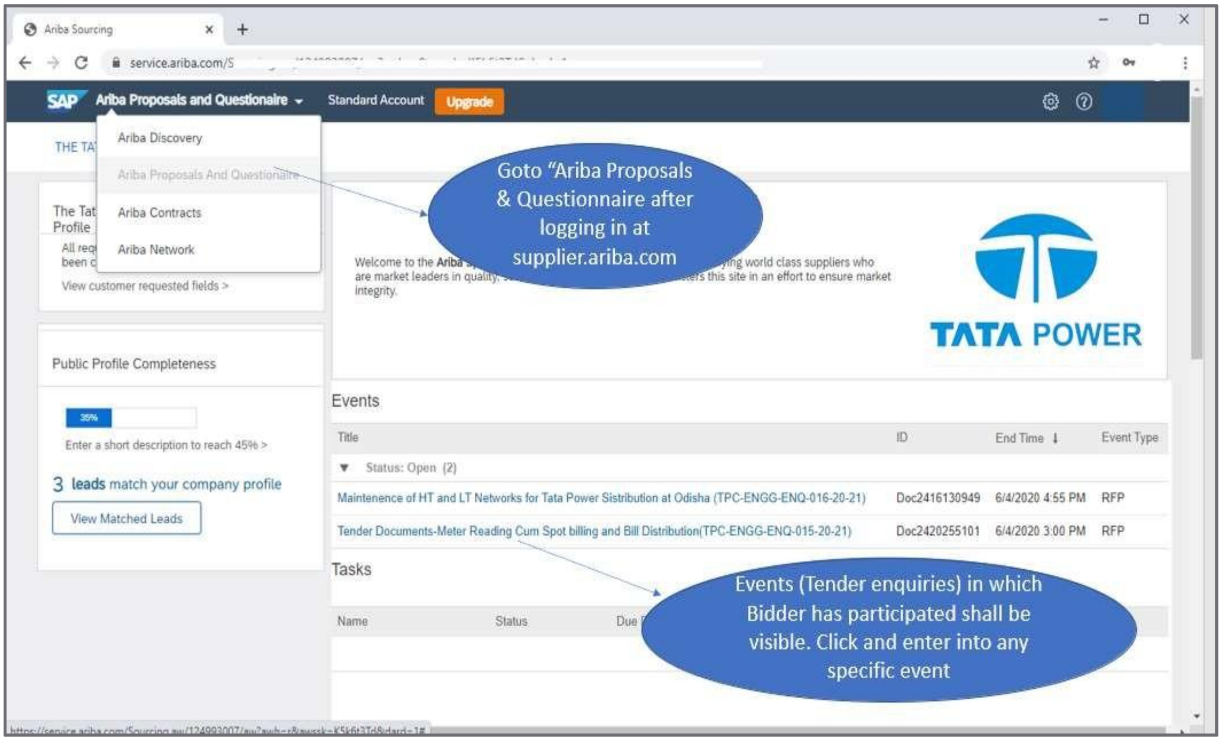
Step 1 - Log on **supplier.ariba.com**

Step 2 - Put your USER ID and Password in following screen



SAP Ariba
Proposals Powered by Ariba Sourcing
Help Center
Supplier Login
User Name
Password
Login
Forgot Username or Password
Need help? See Quick Start

Step 3 - Go to “Ariba Proposals & Questionnaire”.



Goto “Ariba Proposals & Questionnaire after logging in at supplier.ariba.com

Welcome to the Ariba … ing world class suppliers who are market leaders in quality, … ers this site in an effort to ensure market integrity.

Public Profile Completeness

Enter a short description to reach 45% >

3 leads match your company profile

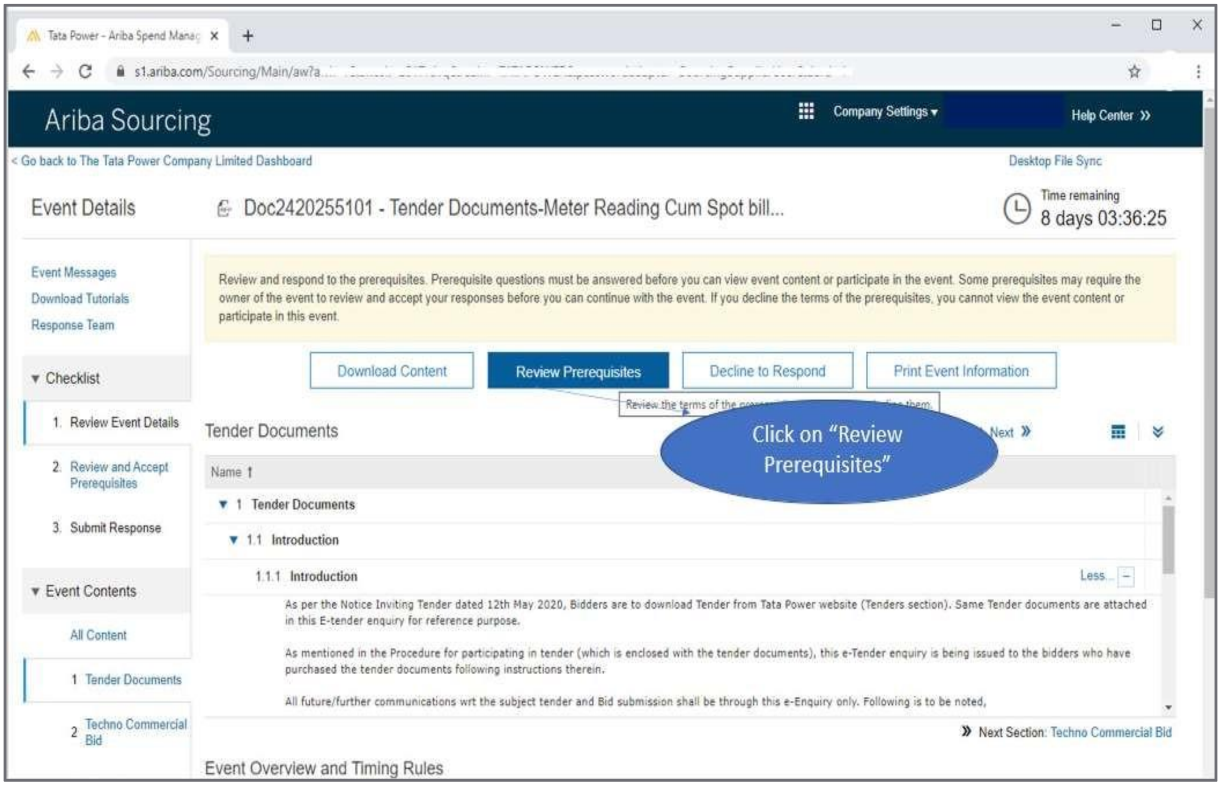
Events

Title	ID	End Time	Event Type
▼ Status: Open (2)			
Maintenence of HT and LT Networks for Tata Power Sistribution at Odisha (TPC-ENGG-ENQ-016-20-21)	Doc2416130949	6/4/2020 4:55 PM	RFP
Tender Documents-Meter Reading Cum Spot billing and Bill Distribution(TPC-ENGG-ENQ-015-20-21)	Doc2420255101	6/4/2020 3:00 PM	RFP

Tasks

Name	Status	Due

Events (Tender enquiries) in which Bidder has participated shall be visible. Click and enter into any specific event



Event Details

Doc2420255101 - Tender Documents-Meter Reading Cum Spot bill...

Time remaining
8 days 03:36:25

Review and respond to the prerequisites. Prerequisite questions must be answered before you can view event content or participate in the event. Some prerequisites may require the owner of the event to review and accept your responses before you can continue with the event. If you decline the terms of the prerequisites, you cannot view the event content or participate in this event.

Review the terms of the … them.

Click on “Review Prerequisites”

▼ Checklist

1. Review Event Details
2. Review and Accept Prerequisites
3. Submit Response

▼ Event Contents

1 Tender Documents
2 Techno Commercial Bid

Tender Documents

Name ↑

▼ 1 Tender Documents

▼ 1.1 Introduction

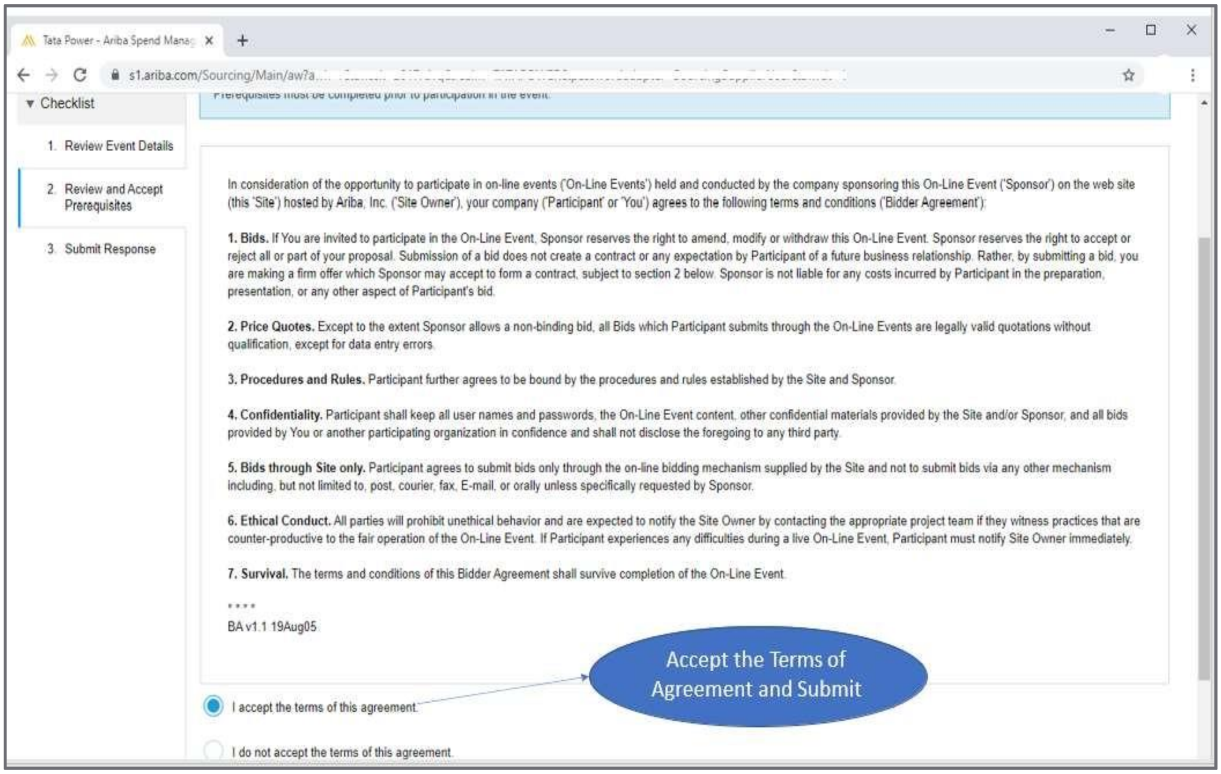
1.1.1 Introduction

As per the Notice Inviting Tender dated 12th May 2020, Bidders are to download Tender from Tata Power website (Tenders section). Same Tender documents are attached in this E-tender enquiry for reference purpose.

As mentioned in the Procedure for participating in tender (which is enclosed with the tender documents), this e-Tender enquiry is being issued to the bidders who have purchased the tender documents following instructions therein.

All future/further communications wrt the subject tender and Bid submission shall be through this e-Enquiry only. Following is to be noted,

Event Overview and Timing Rules


Tata Power - Ariba Spend Manag
s1.ariba.com/Sourcing/Main/aw?a...
▾ Checklist
1. Review Event Details
2. Review and Accept Prerequisites
3. Submit Response

Prerequisites must be completed prior to participation in the event.

In consideration of the opportunity to participate in on-line events ('On-Line Events') held and conducted by the company sponsoring this On-Line Event ('Sponsor') on the web site (this 'Site') hosted by Ariba, Inc. ('Site Owner'), your company ('Participant' or 'You') agrees to the following terms and conditions ('Bidder Agreement'):

1. Bids. If You are invited to participate in the On-Line Event, Sponsor reserves the right to amend, modify or withdraw this On-Line Event. Sponsor reserves the right to accept or reject all or part of your proposal. Submission of a bid does not create a contract or any expectation by Participant of a future business relationship. Rather, by submitting a bid, you are making a firm offer which Sponsor may accept to form a contract, subject to section 2 below. Sponsor is not liable for any costs incurred by Participant in the preparation, presentation, or any other aspect of Participant's bid.

2. Price Quotes. Except to the extent Sponsor allows a non-binding bid, all Bids which Participant submits through the On-Line Events are legally valid quotations without qualification, except for data entry errors.

3. Procedures and Rules. Participant further agrees to be bound by the procedures and rules established by the Site and Sponsor.

4. Confidentiality. Participant shall keep all user names and passwords, the On-Line Event content, other confidential materials provided by the Site and/or Sponsor, and all bids provided by You or another participating organization in confidence and shall not disclose the foregoing to any third party.

5. Bids through Site only. Participant agrees to submit bids only through the on-line bidding mechanism supplied by the Site and not to submit bids via any other mechanism including, but not limited to, post, courier, fax, E-mail, or orally unless specifically requested by Sponsor.

6. Ethical Conduct. All parties will prohibit unethical behavior and are expected to notify the Site Owner by contacting the appropriate project team if they witness practices that are counter-productive to the fair operation of the On-Line Event. If Participant experiences any difficulties during a live On-Line Event, Participant must notify Site Owner immediately.

7. Survival. The terms and conditions of this Bidder Agreement shall survive completion of the On-Line Event.

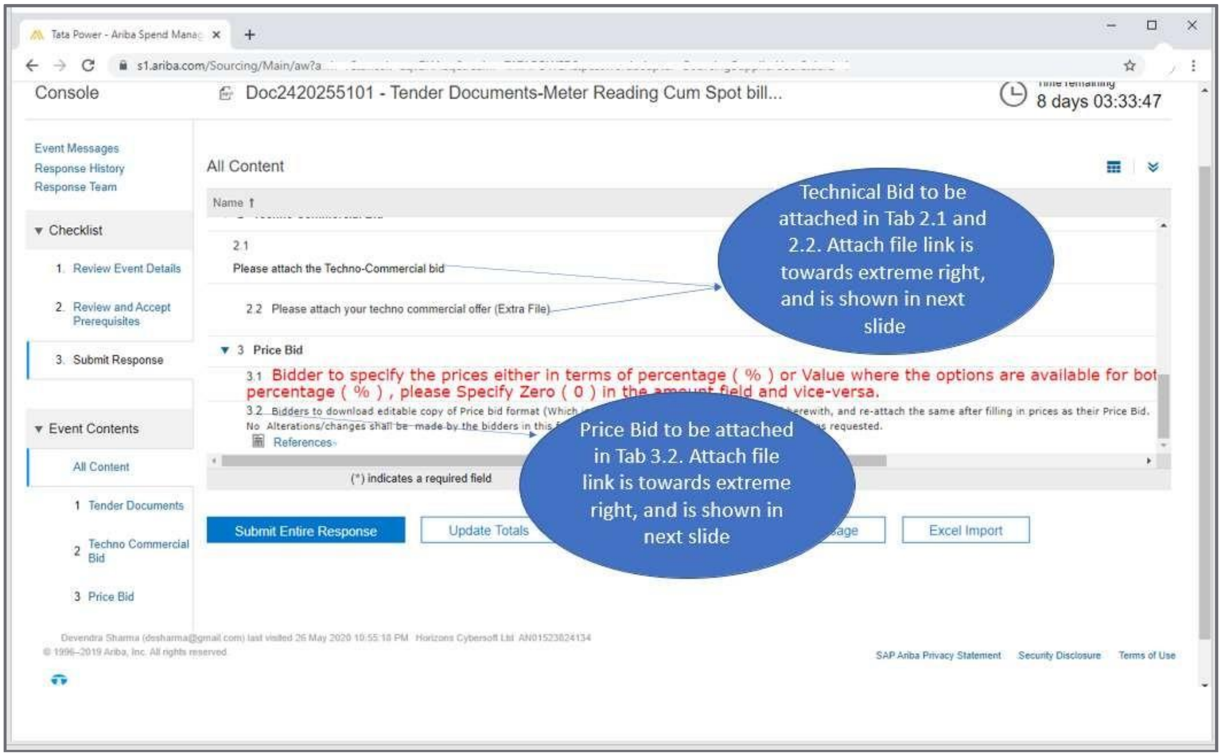
****

BA v1.1 19Aug05

● I accept the terms of this agreement.

○ I do not accept the terms of this agreement.

Accept the Terms of Agreement and Submit



2.1 Please attach the Techno-Commercial bid

2.2 Please attach your techno commercial offer (Extra File)

▾ 3 Price Bid

3.1 Bidder to specify the prices either in terms of percentage (%) or Value where the options are available for bot percentage (%) , please Specify Zero (0) in the amount field and vice-versa.

3.2 Bidders to download editable copy of Price bid format (Which ... herewith, and re-attach the same after filling in prices as their Price Bid. No Alterations/changes shall be made by the bidders in this ... requested.

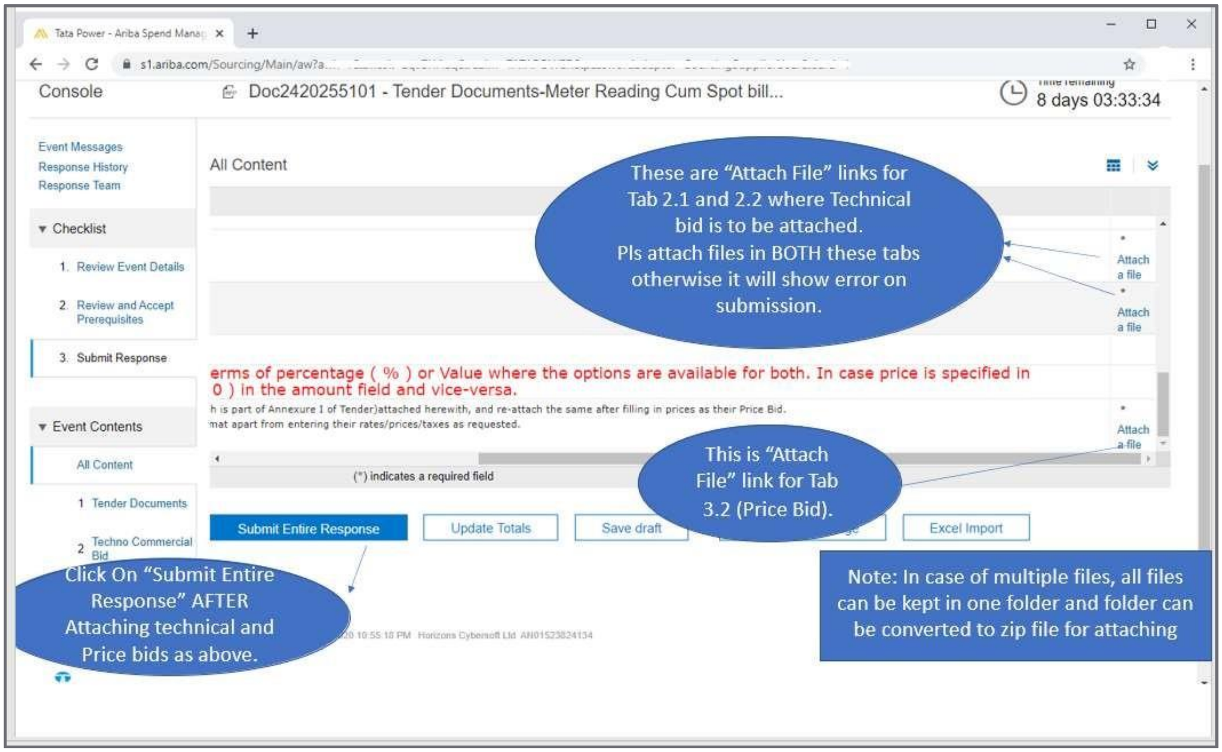
References

(*) indicates a required field

Devendra Sharma (desharma@gmail.com) last visited 26 May 2020 10:55:18 PM Horizons Cybersoft Ltd AN01523824134
© 1996–2019 Ariba, Inc. All rights reserved

Technical Bid to be attached in Tab 2.1 and 2.2. Attach file link is towards extreme right, and is shown in next slide

Price Bid to be attached in Tab 3.2. Attach file link is towards extreme right, and is shown in next slide



erms of percentage (%) or Value where the options are available for both. In case price is specified in 0) in the amount field and vice-versa.

h is part of Annexure I of Tender)attached herewith, and re-attach the same after filling in prices as their Price Bid.
mat apart from entering their rates/prices/taxes as requested.

These are "Attach File" links for Tab 2.1 and 2.2 where Technical bid is to be attached.
Pls attach files in BOTH these tabs otherwise it will show error on submission.

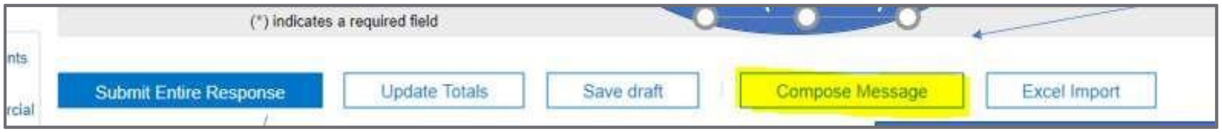
This is "Attach File" link for Tab 3.2 (Price Bid).

Click On "Submit Entire Response" AFTER Attaching technical and Price bids as above.

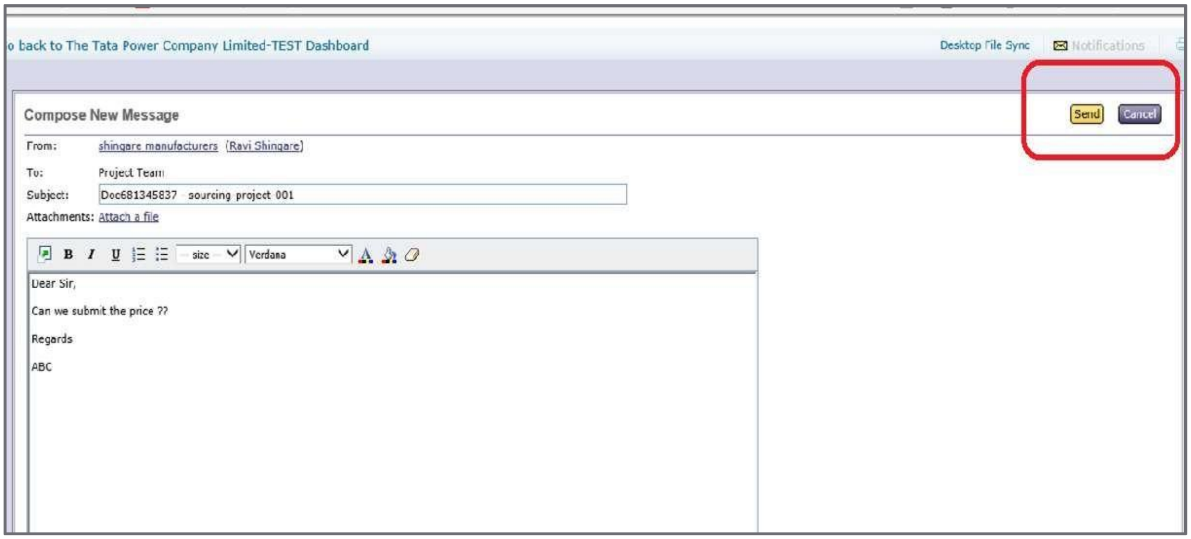
Note: In case of multiple files, all files can be kept in one folder and folder can be converted to zip file for attaching

3 Communicating with Tata Power Buyer during e- bidding

Step 1: Click "Compose Message".



Step 2: Compose Your Message and click "Send".



Compose New Message

From: shingare manufacturers (Ravi Shingare)

To: Project Team

Subject: Doc681345837 sourcing project 001

Attachments: Attach a file

Dear Sir,

Can we submit the price ??

Regards

ABC

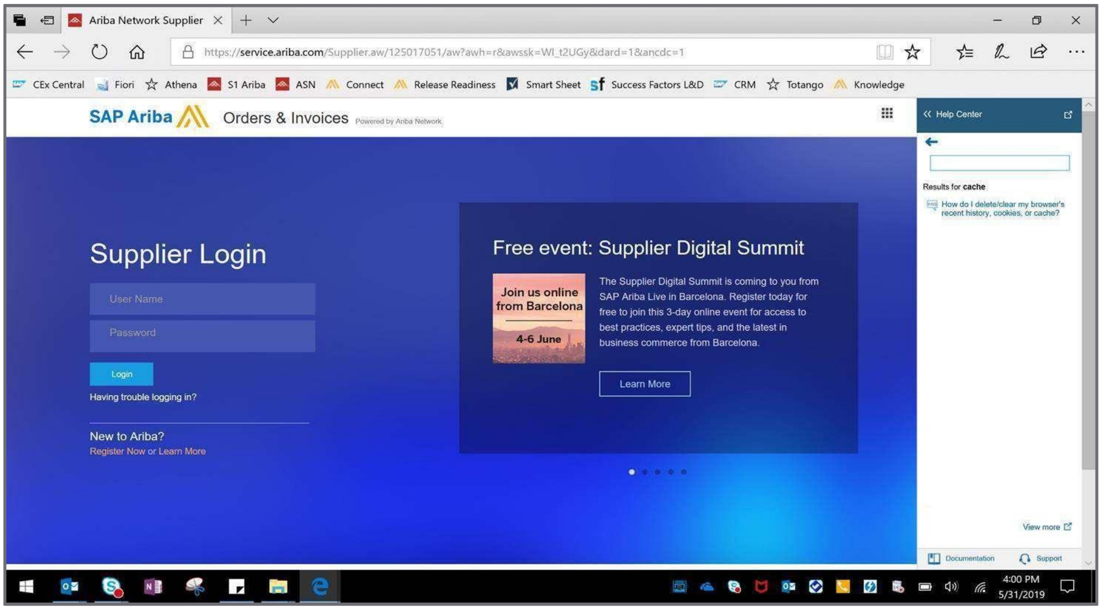
ARIBA TRAINING VIDEOS

[Participating in a RFI or RFP on Ariba Network](https://www.youtube.com/watch?v=9_XXUaVyI7o) - https://www.youtube.com/watch?v=9_XXUaVyI7o

Support from Ariba - Supplier can raise the Ticket for "Support"

Here are the steps that Suppliers can follow for raising a ticket or requesting a call back from Support team. They can do so without logging in – pls follow the brief instructions given below.

1. Go to login page>Choose "Support" on the bottom right corner



https://service.ariba.com/Supplier.aw/125017051/aw?awh=r&awssk=WI_t2UGy&dard=1&ancdc=1

Supplier Login

Free event: Supplier Digital Summit

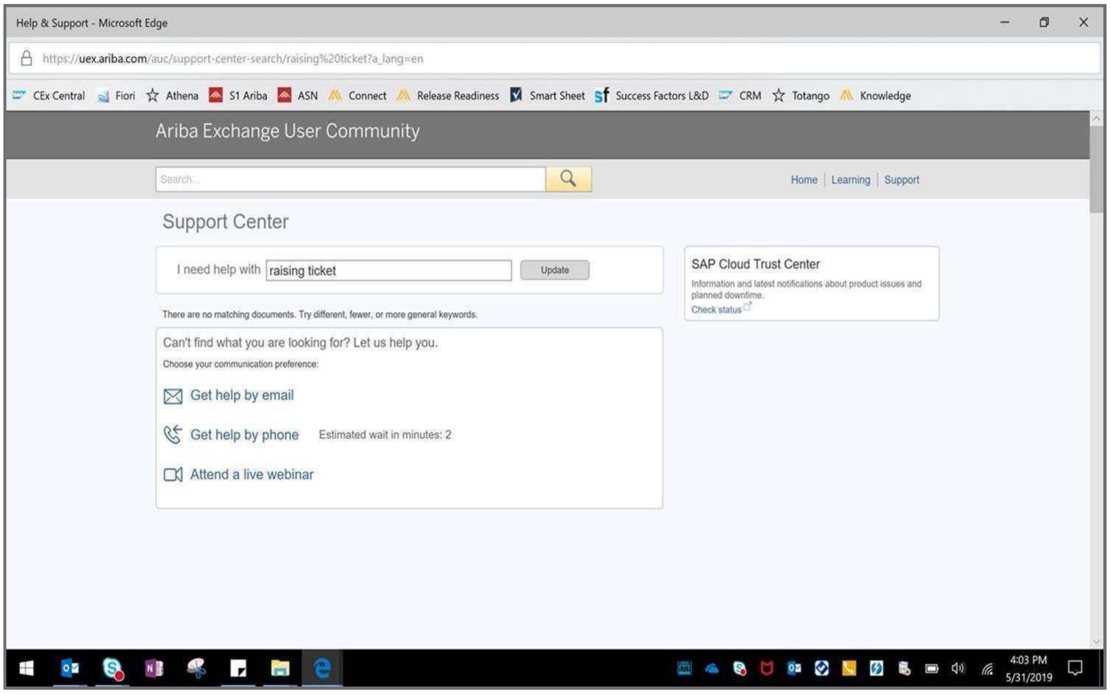
Join us online from Barcelona 4-6 June

The Supplier Digital Summit is coming to you from SAP Ariba Live in Barcelona. Register today for free to join this 3-day online event for access to best practices, expert tips, and the latest in business commerce from Barcelona.

Results for cache

How do I delete/clear my browser's recent history, cookies, or cache?

2. Add query and press "Start" – After that, following screen will pop up where you can choose either Get Help by Email or Get Help by Phone.



https://uex.ariba.com/auc/support-center-search/raising%20ticket?a_lang=en

Support Center

I need help with raising ticket

There are no matching documents. Try different, fewer, or more general keywords.

Can't find what you are looking for? Let us help you.

Choose your communication preference:

Get help by email

Get help by phone Estimated wait in minutes: 2

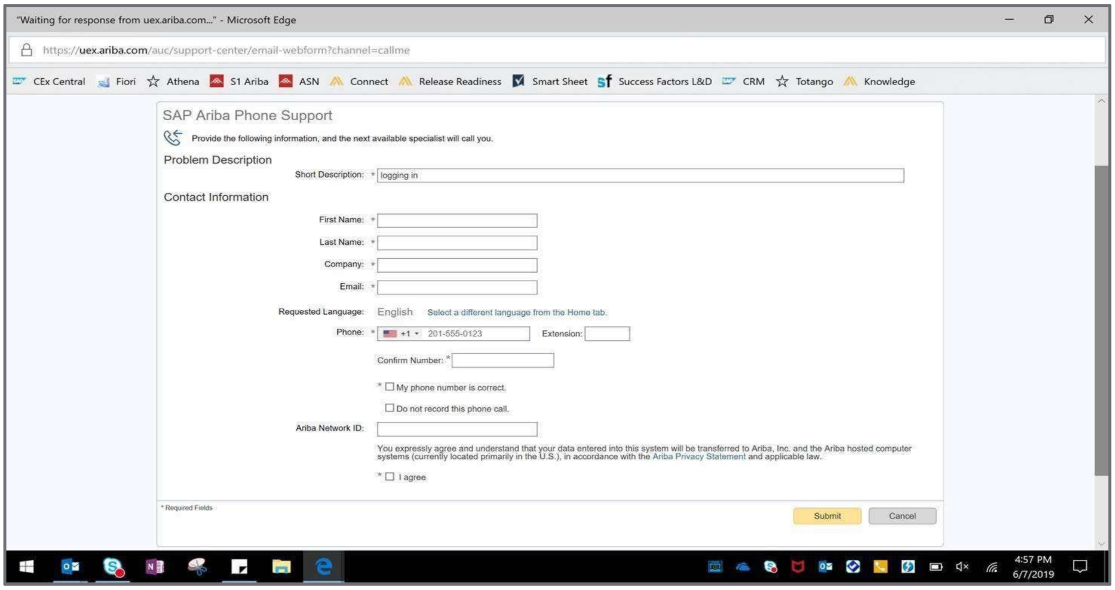
Attend a live webinar

SAP Cloud Trust Center

Information and latest notifications about product issues and planned downtime.

Check status

3. Choose phone and add following basic details and you will get call back



"Waiting for response from uex.ariba.com..." - Microsoft Edge

https://uex.ariba.com/auc/support-center/email-webform?channel=callme

SAP Ariba Phone Support

Provide the following information, and the next available specialist will call you.

Problem Description

Short Description: * logging in

Contact Information

First Name: *

Last Name: *

Company: *

Email: *

Requested Language: English Select a different language from the Home tab.

Phone: * +1 201-555-0123 Extension:

Confirm Number: *

* □ My phone number is correct.

□ Do not record this phone call.

Ariba Network ID:

You expressly agree and understand that your data entered into this system will be transferred to Ariba, Inc. and the Ariba hosted computer systems (currently located primarily in the U.S.), in accordance with the Ariba Privacy Statement and applicable law.

* □ I agree

* Required Fields

If not by phone, they can ask for a response/support by email.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

SUPPLIER FREQUENTLY ASKED QUESTIONS

- **If I registered on my buyer's Ariba Sourcing site in the past, do I need to register again?**

Answer- Yes. Although you have registered on your buyer's Ariba Sourcing site in the past, registering on the Ariba Commerce Cloud is required. The registration process only takes a few moments, with a simple one-page registration. Registering on the Ariba Commerce Cloud gives you access to all your buyer relationships with one username and password.

- **What is the Ariba Commerce Cloud?**

Answer: - The Ariba Commerce Cloud is your entry point to all of your seller solutions.
Rather than managing log in information for multiple buyers' sites, you will have one log in and one account. This means fewer passwords to remember, easier user maintenance for your company, and a unified profile for your organization.

- **Do I need to add Product and Service Categories during registration?**

Answer:-Yes; this is a required field. Product and Service Categories classify what your company sells, and the system uses this information to match potential business opportunities with your products and services.

Click **Add Product and Service Categories** to select one or more categories from the list of options. During registration, you only need to choose one category, preferably related to the event you are joining. You can add, refine, or remove categories any time after the registration process.

- **Do I need to add ship-to or service locations during registration?**

Answer: - Yes; this is a required field. Ship-to or Service locations inform buyers where your company sells its products or provides its services, and the system uses this information to match potential business opportunities with your products and services.

Click **Add Ship-to or Service Locations** to select one or more sales territories from a list. You can add, refine, or remove ship-to or service locations any time after the registration process.

Additional Information: - D-U-N-S is a registered trademark of Dun & Bradstreet or its subsidiaries in the United States and other countries.

- **What is the difference between the Email and Username fields in my profile?**

Answer: - The Email field represents the email address where you wish to receive email notifications. The Username field is the identifier that you use to access your account. The Username field must be in email format, but you do not have to use a valid email address.

Note: Leave the **This is my username** box checked if you want your email address to be the same as your username.

- **How do I participate in my buyer's event using an email invitation?**

Answer: - Use the **Click here** link in the email notification to access the sourcing event.

While buyers might customize the email content you receive, all email invitations contain a link to access the event.

Depending on your previous experience with Ariba solutions, do one of the following to access the event after you click the link:

- If you are new user, click **Continue** on the welcome page. You continue to register an Ariba account to link with your buyer and participate in the event.
- If you have used Ariba before and have already accessed an event for the buyer-specific account with your current log in ID, click the **Login** button to continue. Log in with your Ariba username and password in order to participate in the event.
- If you already have an existing Ariba Network, Ariba Discovery, or Ariba Sourcing supplier account, but you have not accessed any events for the inviting buyer's site, use the **Click here if you already have an Ariba Commerce Cloud, Ariba Discovery or Ariba Network account** link. After clicking the link, log in with your existing account to move your information to your buyer's site.

Additional Information:- Registering an Ariba account provides you with a consolidated view of all your customer relationships. With this one profile, you can view business opportunities, participate in sourcing events, participate in contract negotiations, and manage orders, catalogs, and invoices.

- **Why doesn't the link in the email invitation to participate in a sourcing event work?**

Answer:-If you cannot click the link, or the link does not open the log in page, highlight and copy the Uniform Resource Locator (URL), and then paste the URL into your web browser.

- **Can my company have multiple accounts?**

Answer:-Your Company can have multiple Ariba accounts, depending on your business needs. For example, if your company has several locations around the world, you might want a separate account for each region.

Most companies choose to have one account with multiple customer relationships, which provides a centralized location to maintain their company profile information and all of their customer relationships.

How do I complete registration if my username already exists?

Answer: - This message means that you already have an Ariba Network, Ariba Discovery, or Ariba Sourcing supplier account registered under username you entered. You can either register ua new account by creating a new username, or access one of the following sites to request a password reset for the registered username:

- Ariba Network (This login page is used for all Ariba Network, Ariba Sourcing, or Ariba Contracts suppliers).
- Ariba Discovery login page

To reset your password, click the **Having trouble logging in?** Link on the Login page.

Nothing happens when I click Forgot Username and enter my email address

Issue: - Nothing happens when I click the **Forgot Username** link and enter my email address.

Cause: - After you submit your request to retrieve your username, the Ariba Network sends an email notification with usernames that match the email address you submitted.

Some possible reasons why you may not receive this username retrieval email notification:

- The email address on your account does not match the email address you entered when submitting the request.
- Your buyer-specific account was deactivated before you could move it to the Ariba Commerce Cloud. Generally, that means you probably have not participated in an event with that buyer for a while.

Solution: -

- To ensure you receive this email notification:
- Make sure you type the email address configured within your account.

If your buyer-specific account has been deactivated, contact your buyer to determine how to proceed.

Where is my password reset email?

Answer: - After you submit your request for a password reset, Ariba sends instructions to the email address associated with your account. If you didn't receive a password reset email, check the following scenarios to troubleshoot.

The username you entered is in the wrong format, or it isn't associated with the email address you are checking.

- Keep in mind, your username is in the format of a full email address, but it can be associated with any email address you entered previously.
- Your username is also case-sensitive.
- To confirm that you are using the correct username and format, return to the Ariba login page, and click the **Having trouble logging in?** link (**Forgot Username** if you're working in Ariba Discovery).
  - Choose **I forgot my username**, and click **Continue**.
  - Enter the email address associated with your account, and click **Submit**.

    - You will receive an email that lists the exact format of the username associated with the email you entered.

You entered the correct username, but you still didn't receive the password reset email notification.

- This can occur if the configured email address is different from the account you are checking.
- You might have multiple accounts for your company, so make sure you are attempting to access the correct account.

Your email configuration or company's security settings might also prevent you from receiving the password reset email. To find out, check your junk mail folder or email filter settings to verify that automated emails from Ariba are not blocked from your email account.

- **Why do I get this message on the SAP Ariba Login page: "The username and password pair you entered was not found"?**

Answer: - You entered an incorrect **Username** or **Password**. You might receive this message if you entered a previous **Username** or **Password**. Remember that your **Username** has the format of an email address, and both the **Username** and **Password** are case sensitive.

Click the **Having trouble logging in?** Link on the Login page if you don't remember your log in information.