BSES
RAJDHANI POWER LIMITED

TENDER NOTIFICATION FOR

Implementation of Security Operations Center in BRPL

NIT NO: CMC/BR/25-26/FK/PR/KB/1239

Tender Date: 21.01.2025

Due Date for Submission: 10.02.2025; 1500 Hrs.

BSES RAJDHANI POWER LTD (BRPL)
Corporate Identification Number: **U74899DL2001PLC111527**
Telephone Number: +91 11 3009 9999
Fax Number: **+**91 11 2641 9833
Website: **www.bsesdelhi.com**

BSES
RAJDHANI POWER LIMITED

S.No.	ITEM	DESCRIPTION
1.	**CHECK LIST**	CHECK LIST FOR BID SUBMISSION
2.	**SECTIONS**	
2.1	SECTION-I	REQUEST FOR QUOTATION (RFQ)
2.2	SECTION-II	INSTRUCTION TO BIDDERS (ITB)
2.3	SECTION-III	SPECIAL CONDITIONS OF CONTRACT (SCC)
2.4	SECTION-IV	GENERAL CONDITIONS OF CONTRACT (GCC)
2.5	SECTION-V	SCOPE OF WORK
2.5	SECTION-VI	PRICE BID
2.6	SECTION-VII	VENDOR CODE OF CONDUCT
3.	**APPENDIX**	
3.1	APPENDIX-I	COMMERCIAL TERMS AND CONDITIONS – SUPPLY
3.2	APPENDIX-II	NO DEVIATION DECLARATION
3.3	APPENDIX-III	BID FORM
3.4	APPENDIX-IV	ACCEPTANCE FORM FOR PARTICIPATION IN REVERSE AUCTION EVENT
3.5	APPENDIX-V	FORMAT FOR EMD BANK GUARANTEE
3.6	APPENDIX-VI	LITIGATION HISTORY
3.7	APPENDIX-VII	CURRENT CONTRACT COMMITMENTS/ WORK IN PROGRESS
3.8	APPENDIX-VIII	FINANCIAL DATA
3.9	APPENDIX-IX	FORMAT FOR PERFORMANCE BANK GUARANTEE
3.10	APPENDIX-X	FORMAT FOR PRE BID QUERY SUBMISSION
3.11	APPENDIX-XI	NO-DISCLOSURE AGREEMENT (NDA)
3.12	APPENDIX-XII	BIDDER'S COMMUNICATION DETAILS

BSES
RAJDHANI POWER LIMITED

CHECK LIST

(FOR BID SUBMISSION)

S. No	Item Description	Yes/ No
1	BID INDEX	
2	COVERING LETTER	
3	CHECK LIST	
3	TENDER FEE	
4	EARNEST MONEY DEPOSIT	
5	POWER OF ATTORNEY	
6	BID FORM DULY SIGNED	
7	NON-DISCLOSURE AGREEMENT (NDA)	
8	NO DEVIATION DECLARATION (NDD)	
9	UNPRICED TECHNO-COMMERCIAL BID (IN SEPARATE SEALED ENVELOPE-1)	
10	PRICE BID (IN SEPARATE SEALED ENVELOPE-2)	
11	COMPLETE BID DOCUMENTS, ENVELOPE 1 & 2 (IN SEPARATE SEALED ENVELOPE-3)	
12	APPENDIX I-XII	

RAJDHANI POWER LIMITED

SECTION- I
REQUEST FOR QUOTATION (RFQ)

BSES
RAJDHANI POWER LIMITED

SECTION- I
REQUEST FOR QUOTATION (RFQ)

1. GENERAL

1.1. BSES Rajdhani Power Limited invites sealed tenders on a "Single Stage: Two Envelope" bidding basis (Envelope –I, Techno-Commercial Bid & Envelope-II, Price Bid) from eligible Bidders for " Implementation of Security Operations Center in BRPL". The bidder must qualify the requirements as specified in heading "Qualifying Requirements" of this RFQ.

1.2. The sealed envelopes shall be duly super-scribed as:

NIT NO: CMC/BR/25-26/FK/PR/KB/1239 Dated: 21.01.2025

For

Implementation of Security Operations Center in BRPL

1.3. Schedule of the tendering process is given below. Detailed Specification, Scope of Work, Terms & Conditions, etc are mentioned in the Tender documents, which is available on our website.

Cost of Tender Documents (Non- Refundable)	Rs.1180/- (including GST)
Estimated Cost (Rs) with GST	Rs. 5.38 Cr (including GST)
Earnest Money Deposit	Rs. 5,38,000/-
Delivery & Installation at	BRPL Store/Sites
Delivery Schedule / period	Within 45 Days from date of PO / LOI
Tender documents on sale	21.01.2025
Date & time of Submission of Bid	10.02.2025; 1500 Hrs
Date & time of opening of Techno-Commercial Bid	10.02.2025; 1530 Hrs

1.4. The tender document can be obtained from address given below against submission of non-refundable demand draft of **Rs.1180/-** drawn in favour of BSES Rajdhani Power Ltd, payable at Delhi:

Head of Department
Contracts & Material Dept.
BSES Rajdhani Power Limited
Ist Floor, Tender Room, BSES Bhawan
Nehru Place, New Delhi -110019.

The tender documents & detail terms and conditions can also be downloaded from the website **"www.bsesdelhi.com --> Tenders --> BSES Rajdhani Power Ltd --> Open Tenders"**.

In case tender papers are downloaded from the above website, then the bidder has to enclose a demand draft covering the cost of bid documents.

1.5. Only DD shall be accepted for tender fees.

1.6. The tender documents will be issued on all working days up to the date mentioned in clause 1.3. The tender documents & detail terms and conditions can also be downloaded from the website www.bsesdelhi.com. In case tender documents are downloaded from the above website, then the bidder has to enclose a separate demand draft covering the cost of bid documents.

2. POINTS TO BE NOTED

2.1. Works envisaged under this contract are required to be executed in all respects up to the period of completion/ duration of work mentioned above.
2.2. Only those agencies, who fulfilll the qualifying criteria as mentioned in clause 3 should submit the tender documents.
2.3. BSES Rajdhani Power Ltd reserves the right to accept/reject any or all bids without assigning any reason thereof and alter/amend/modify/add/reduce the amount and quantity mentioned in the tender documents at the time of placing Order
2.4. The bid will be summarily rejected if:
(a) **Earnest Money Deposit (EMD)** and **Tender Fee** of requisite amount is not deposited as per tender conditions
(b) Bid received after due date and time.
(c) Complete technical details are not enclosed
(d) Technical offers contains any prices
e) The offer does not contain prices indicating break-up towards all taxes & duties in prescribed format
f) Prices are not firm and subject to Price Variation

3. EMD

3.1. The bidder shall furnish, as part of its bid, an EMD of the requisite amount. The EMD is required to protect the Company against the risk of Bidder's conduct which would warrant forfeiture. The EMD shall be denominated in any of the following forms:

(a) BG from nationalized / Scheduled Bank, as per the format annexed in the tender document, in favour of BSES Rajdhani Power Limited valid for 6(six) months from original due date of bid submission.
(b) Fixed Deposit (lien marked in favor of BSES RAJDHANI POWER LTD) valid for 6(six) months from original due date of bid submission.

3.2. Please note that bank details as given below have been provided only for the purpose of making BG for EMD.

Beneficiary Name	: BSES Rajdhani Power Limited
Bank Name	: State Bank of India (SBI)
A/c No.	: 40214783615
IFSC Code	: SBIN0009601

3.3. The EMD of the bidders who are not technically qualified shall be returned after the price bid opening.

3.4. Earnest money given by all the bidders who are techno commercially qualified except the lowest bidder shall be returned within 8 (Eight) weeks after award of the work.

3.5. The EMD of the successful bidder shall be returned on submission of Performance Bank Guarantee (PBG) as per tender terms.

3.6. The EMD may be forfeited in case of:
- a) The Bidder withdraws its bid during the period of bid validity specified by the Bidder in the Bid Form or
- b) The successful Bidder does not
  - (i) accept the Purchase Order/Purchase order, or
  - (ii) furnish the required PBG as per tender terms
- c) The bidder is found to have submitted false or forged, any of the documents/ certificates/ information.

4. QUALIFYING REQUIREMENTS (QR)

The prospective bidder must qualify all of the following requirements to be eligible to participate in the bidding. Bidders who meet following requirements will be considered as successful bidder and management has a right to disqualify those bidders who do not meet these requirements.

Technical QR:

S. No.	Criteria	Documents to be submitted by the bidder
1.	The Bidder should be OEM or Authorized channel Partner of the OEM as on the date of tender with an authority to sale, upgrade, supply, service and maintain the proposed products.	In case bidder is an authorized partner of OEM, Manufacturer Authorization Form (MAF) from OEM stating that bidder is an authorized partner of OEM and authorized to participate in this tender.
2.	The Bidder should be a Managed Security Service Provider (MSSP) having its own Security Operations Centre (SOC) operating since last 4 years from the date of bid submission, from where it is providing services to different customers	Self-declaration by bidder along with Client name, contact details and project details
3.	The bidder's company should have been in existence for more than 7 years and bidder/ OEM must have experience of project execution of similar work as per tender requirement in Govt sector/ power sector/ energy/ BFSI/ critical sector in last 4 years.	Certificate of Incorporation Self-declaration by Authorized bidder or OEM along with Client name and project details. If bidder is an authorized partner of OEM, credentials of OEM shall be considered for similar project execution experience.
4.	Bidder should have experience of SOC operations for minimum 5 SOC customers in last 4 years in Govt sector, power sector, energy, BFSI or critical sector. Customer names on bidder letter head along with person's name, contact details like mail id and phone numbers to be provided.	Self-declaration by bidder along with Client name, Contact person, Phone no. , Email Id, project details.

5.	Bidder must have at least 3 deployments for 20000 EPS installation, each in Govt sector/ power sector/ energy/ BFSI/ critical sector (period ending bid submission date) for proposed SIEM solution or Must have at least 1 deployment for 75000 or more EPS installation in Govt sector, power sector, energy, BFSI or critical sector (period ending bid submission date) for proposed SIEM solution	a. Purchase Order copies b. Performance Certificate/ Completion certificate/ Invoice Copies If bidder is an authorized partner of OEM, credentials of OEM shall be considered.
6.	OEM/Authorized channel partner's country shall not share land border with India as per MoP Order no. No.25-11/6/2018-PG dated 2 July, 2020 and Order No.25-4.1.2019-PG dt.11Aug, 2020.	Self-undertaking on bidder's letterhead
7.	Bidders should have Latest valid ISO 27001 certification as on bid submission date	Bidder should furnish the copies of Valid Certificate

Financial QR:

(i) The average annual turnover of the Bidder, in the preceding three (3) financial years (i.e., FY23-24, FY22-23 & FY21-22) should not be less than Rs 11 Crore. The bidder shall submit the Annual Turnover Report of the last 3 FYs duly certified by a Chartered Accountant. The Turnover certificate must have UDIN Number.

(ii) The bidder should have net worth of Rs 2 Crore as on the last day of the preceding financial year on the date of bid submission. The bidder shall submit the Certificate of Net Worth duly certified by Chartered Accountant for the last financial year i.e. FY 2023-24. The Net worth certificate must have UDIN Number.

(iii) Bidder must provide proof of having solvency of an amount equal to Rs 1.5 Crore from any nationalized/ scheduled commercial bank. It should not be older than 30 days from the date of submission of Techno-Commercial bid.

(iv) Bidder should have valid Registration of GST & PAN.

(v) Bidder should fulfil all statutory compliances like PF, ESI registration, etc.

(vi) Entities that have been currently debarred/blacklisted by any Private/central/state government institution including electricity boards in India, any of the DISCOM in India, lacks qualifying pre-requisites to participate in this tender will not be considered. Accordingly an undertaking by the Authorized Person along with other documents to be provided by the bidder on its letter head in this regard, confirming in clear terms, that the contractor has not been debarred/blacklisted as on the date of submission of the bid. Bidders who is currently debarred/ blacklisted/ suspended by BRPL will not be considered in this tender.

(vii) The bidder should give an undertaking by the Authorized Person on their letterhead that all the documents/certificates/information submitted by them against the tender are genuine/true/correct and the copies of documents have been made from the original document/s. Further, in case any of the documents/certificates/information submitted by the bidder is found to be false or forged, BRPL at its sole discretion shall be free to take all actions as permitted under law, including forfeiture of EMD and disqualification from participation in the future tenders of BRPL & Its group companies for indefinite period or period as may be decided by BRPL.

(viii) The bidder should submit an undertaking for "No Litigation" / no legal case is pending with BRPL or its Group Companies. Bidders having any litigation/ legal case pending with BRPL shall not be considered qualified for this tender.

Other Requirements:

(a) Company reserves the right to carry out technical capability/ infrastructure assessment of the Bidders by factory/office/site inspection or by any other means and company's decision shall be final in this regard.

(b) The bidder shall submit all necessary documentary evidence to establish that the Bidder meets the above qualifying requirements including but not limited to following:

i. Last three Financial Years (FY 21-22, FY 22-23 & FY 23-24) audited financial statement along with UDIN based CA certificate.
ii. Bidder to submit UDIN based CA Certificate showing NIL dues towards Statutory Liabilities, including GST, Taxation, PF, ESI, or any other dues Statutory in nature for the period upto 30.06.2024, herein collectively called as "Statutory dues" and there is no liability over the bidder relating to deposition of such statutory dues.
iii. Detail of Banks & Fund & Non fund based Credit limit
iv. Details of formation/registration of the firm (Proprietary/ Partnership) or Company along with all relevant details)
v. Memorandum & Articles of Association of the Company/ Partnership Deed of the Firm /other registration documents, as applicable
vi. Organization Chart of the Bidders Company/organisation
vii. Organisation chart for execution of the contract comprising of qualified manager, Safety officer, HR manager, Technicians / Diploma / Graduate Engineers etc.
viii. Experience details with credentials
ix. Number of Employees & necessary details
x. Details of office/s in Delhi/NCR. Details of Registered and Corporate offices and details of other offices/establishments in India.
xi. Work order copies along with performance certificates in support of relevant experience
xii. Turnover certificate issued by CA (along with UDIN no.) for the last three Financial Years.
xiii. Networth certificate as elaborated in financial QR

xiv. List of pending litigation with government/other institution on account of executing any order.
xv. Copy of ESI/PF Registration certificate
xvi. Copy of PAN/GST no.
xvii. Copy of GST Return of last Financial Year.
xviii. Non-Disclosure Agreement (NDA) as per format attached
xix. Bidder's details as per format attached
xx. Solvency Certificate.
xxi. The bidder should enclose performance certificates in support of relevant experience.

(c) For existing vendors of BRPL, the evaluation will also include the performance in the existing contracts via-a-vis performance in terms of HR issues, all statutory Compliance parameters and wages disbursement by Vendors. BRPL reserves the right to qualify or disqualify their bid based on the contract performance despite them meeting the above-mentioned qualification requirements.

BRPL may ask for such other documents as it deems fit for substantiating/ justifying the submissions made by the bidder.

Bidders already qualified against previous tenders for similar requirement ALSO NEED TO SUBMIT the documents in support of qualification criteria.

5. PRE-BID MEETING:

A pre-bid meeting shall be organized at the 30.01.2025; 14:30 HRS as specified in the tender documents in the presence of those bidders or their authorized representatives who may choose to be present.

Location for Pre-Bid meeting:

BSES Rajjdhani Power Limited,
BSES Bhawan, 2nd Floor,
Ganga Conference Room
New Delhi – 110019
Date: 30.01.2025
Time: 02:30 PM onwards

All queries related to this tender must reach to C&M Department of BRPL at least three days before the date of the pre-bid meeting in pre-bid format (APPENDIX-X) vide email as mentioned below:

For Technical:
Shaleen.khetrapaul@relianceada.com
Cc: Nitin.galande@relianceada.com
For Commercial:
Kuber.bhatia@relianceada.com
Cc: **bhaskar.chattopadhyay@relianceada.com**

All the bidder's queries shall be replied to in the pre-bid meeting. In case any change is required in the tender document the same shall be affected in the form of corrigendum to this tender. The bidder or their representatives who intend to bid and who have either purchased tender documents or will pay tender fees for downloaded documents are invited to attend the pre-bid meeting. Corrigendum, if any, to the tender document shall be hosted on the website subsequent to the pre-bid meeting. Bidders are requested to submit their offer strictly in line with this tender document & corrigendum if any.

6. BID SUBMISSION

6.1. The bidders are required to submit the bid in 2(two) parts and in original & duplicate (total 2 copies) at the following address:

Head of Department,
Contracts & Material Department,
BSES Rajdhani Power Limited,
Ist Floor, Tender Room,
BSES Bhawan, Nehru Place,
New Delhi-110019.

6.2. Technical bid documents along with commercial terms and conditions shall also be submitted in Pen Drive. **No price bid shall be submitted in Pen Drive.** The PEN Drive should be owned by Bidder. The bidder shall ensure that the Pen Drive is free from all viruses/malware. The pen drive once submitted shall not be returned.

6.3. This is a two part bid process. Bidders are to submit the bids in 2(two) parts. Both these parts should be furnished in separate sealed covers super scribing **NIT no. DUE DATE OF SUBMISSION, with particulars as PART-A Techno-Commercial Bid and Part-B PRICE BID** and these sealed envelopes should again be placed in another sealed envelope which should be super scribed with **—"Tender Notice No.& Due date of opening".** The same shall be submitted before the due date & time specified.

6.3.1 PART A: TECHNO-COMMERCIAL BID, UNPRICED (Envelop-1):

The first sealed envelope shall contain an Unpriced Techno-commercial bid in paper form (hard copies) and envelope super-scribing **PART-A Techno-Commercial Bid**. The details to be submitted in techno-commercial bids are given below:

a) General information about bidder
b) Documentary evidence in support of all the qualifying criteria as per clause 4.0,
c) EMD of requisite amount
d) Non-refundable separate demand draft for Rs. 1180/- In case the forms are downloaded from the website
e) Technical Literature if any.
f) Technical Details / Filled in GTP/Type test report etc
g) Testing Facilities
h) Details of experience of works of the same or similar nature. Copies of Orders, Execution /Performance Certificate & Other Documents to support the QC as per

clause 2.0

i) Power of attorney
j) Acceptance to Commercial Terms and Conditions viz Delivery schedule/period, Payment terms, BG etc
k) No Deviation Declaration
l) Any other relevant document to support bidder meeting QR

m) Original Tender documents duly stamped & signed on each page as token of acceptance
n) Qualified Manpower available & Organization chart

Techno-Commercial Bid should not contain any cost information whatsoever and shall be submitted within the due date. After techno-commercial evaluation, the list of techno-commercially qualified bidders will be posted immediately on the BSES website.

The bidder should submit complete tender document along with all corrigendum (if any) published against this NIT at our website, signed and stamped with bidder's seal as an acceptance of all the terms & conditions of the Tender.

6.3.2 PART B: PRICE BID (Envelop-2):

The second sealed envelope shall contain Price bids in paper form (hard copies and envelope super-scribing **PART-B Price Bid** on it. The details to be submitted in the Price bid are given below:

(a) **PRICE BID** shall Comprise of Prices **strictly** in the Format enclosed in SECTION VI. Any change in price bid format, content may lead to rejection of the bid.

(b) Price Bid will be opened after techno-commercial evaluation of all the bids and only of the qualified bidders.

6.3.3 FINANCIAL BID EVALUATION THROUGH REVERSE AUCTION:

The company reserves the right to conduct Reverse Auction (RA) for finalization of contract hence the details of the price bid shall not be shared with bidders. The qualified bidders will participate in reverse auction through SAP-SRM tool. The RA process shall be governed by the terms and conditions enclosed as Annexure-IV in this tender document. Training/details shall be provided to bidders before participation in auction. In case RA is not conducted /concluded for any reasons, a "final no regret" financial bid in a sealed envelope will be called for from all qualified bidders. Notwithstanding anything stated above, the Company reserves the right to assess bidders' capability to perform the contract, should the circumstances warrant such assessment in the overall interest of the Company. In this regard, the decision of the Company shall be final and binding on the bidders.

Notwithstanding anything stated above, the Purchaser reserves the right to assess bidder's capability to perform the contract, should the circumstances warrant such assessment in the overall interest of the purchaser. In this regard the decision of the purchaser is final.

BIDS RECEIVED AFTER DUE DATE AND TIME MAY BE LIABLE TO REJECTION

7 TIME SCHEDULE

The activities and their timelines are given hereunder which needs to be adhered by the bidders.

S. No.	Activity	Description	Due date
1.	Submission of Technical& Commercial Queries, if any	All Queries related to NIT submit in Pre-bid query format as per APPENDIX-X at kuber.bhatia@relianceada.com Bhaskar.chattopadhyay@relianceada.com	27.01.2025.
2.	Pre-Bid Meeting	Discussion on pre-bid queries	30.01.2025.
3.	Submission of Techno-Commercial & Price Bid	Unpriced Techno-Commercial & Price Bid in separate sealed envelopes	10.02.2025; 1500 Hrs.
4.	Opening of Techno-Commercial Bid	Opening of PART-A	10.02.2025; 1530 Hrs.
5.	Opening of Price Bid	Opening of PART-B of only the techno-commercially qualified bidders (List of bidders will be published at our website)	To be informed separately
6.	Reverse Auction (If required)	As per RA terms	Schedule will be intimated to eligible bidders through email from email id: BRPL.Eauction@relianceada.com

8 AWARD DECISION

8.1. Company intends to award the business on a lowest bid basis, so bidders are encouraged to submit the bid competitively. The decision to place order/LOI solely depends on Company on the cost competitiveness across multiple lots, quality, delivery and bidder ‘s capacity, in addition to other factors that Company may deem relevant.

8.2. The Company reserves all the rights to award the contract to one or more bidders who meet the execution requirement or nullify the award decision without assigning any reason thereof.

8.3. Qty Variation: The Company reserves the rights to vary the quantity by (+/-) 30% of the tender quantity

8.4. In case the performance of any bidder is found unsatisfactory during the delivery process, the award will be cancelled and BRPL reserves the right to award the work to another bidder(s) who will be found eligible/fit.

8.5. The abnormally higher or abnormally lower bids shall not be considered with respect to estimated cost. The criteria decided by BRPL on this shall be final and binding on the bidders.

8.6. The bidding firms are advised to quote their Margin / Administrative Service Charges accordingly. BRPL reserves the right to reject the bids quoted with abnormally higher or abnormally lower individual activity rates. The criteria decided by BRPL on this shall be final and binding on the bidders and will not be open for discussion under any circumstances.

8.7. In the event of your bid being selected by company (and / or its affiliates) and you subsequent DEFAULT on your bid; you will be required to pay purchaser (and / or its affiliates) an amount equal to the difference in your bid and the next lowest bid on the quantity declared in NIT/RFQ.

9 MARKET INTEGRITY

We have a fair and competitive marketplace. The rules for the bidders are outlined in the Terms & Conditions of the tender documents. Bidders must agree to these rules prior to participating in the tender. In addition to other remedies available, we reserve the right to exclude a bidder from participating in future markets due to the bidder's violation of any of the rules or obligations contained in the Terms & Conditions. Bidder(s) who violate the marketplace rules or engage in behavior that disrupts the fair execution of the marketplace restricts a bidder from participation in future tenders of BRPL to a length of time as decided by BRPL, 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 the terms published in Request for Quotation/NIT
- Misrepresentation of facts, submitting false and fabricating documents

10 CONFIDENTIALITY

All information contained in this tender document is confidential and shall not be disclosed, published or advertised in any manner without written authorization from BRPL. This includes all bidding information submitted.

All tender documents remain the property of BRPL and all bidders are required to return these documents to BRPL upon request.

Bidder(s) who do not honor these confidentiality provisions will be excluded from participating in future bidding events.

The bidder shall sign a Non-Disclosure Agreement (NDA) in the format attached in tender document and submit along with its bid.

11 CONTACT INFORMATION

Technical & Commercial clarification, if any, regarding this tender shall be sought in writing and sent by e-mail to the following e-mail IDs:

Address	Name & Designation	E-mail Address / Phone Number
BSES Rajdhani Power Ltd	**Technical**	

C&M Dept, 1st Floor, Tender Room, BSES Bhawan, Nehru Place, New Delhi 110019	Sh Shaleen Khetarpaul (AVP – IT)	**Shaleen.khetrapaul@relianceada.com** /011-49209680
	Sh Nitin Galande (VP – IT)	**Nitin.Galande@relianceada.com** /011-49209745
	All technical queries shall also be marked copy to Commercial team as per the details below.	
	Commercial	
	Mr. Kuber Bhatia GM – (C&M)	**Kuber.Bhatia@relianceada.com** / 011-4920 9955
	Mr. Bhaskar Chattopadhyay AsVP – (C&M)	**Bhaskar.Chattopadhyay@relianceada.com** / 011-4910 7402
	Mr. Amitava Nandi Head(Contracts)– C&M	**Amitava.Nandi@relianceada.com** / 011-4920 9619

***

SECTION-II : INSTRUCTIONS TO BIDDERS (ITB)

1. GENERAL

BSES Rajdhani Power Ltd (BRPL), hereinafter referred to as the “Company” is desirous for awarding work of “Implementation of Security Operations Center in BRPL” as notified in this tender document.

1.1 All the Bids shall be prepared and submitted in accordance with these instructions.

1.2 Bidder shall bear all costs associated with the preparation and delivery of its Bid, and the Company will in no case shall be responsible or liable for these costs.

1.3 The Bid should be submitted by the Bidder in whose name the bid document has been issued and under no circumstances it shall be transferred /sold to the other party.

1.4 The Company reserves the right to request for any additional information/documents and also reserves the right to reject the proposal of any Bidder, if in the opinion of the Company, the data in support of RFQ requirement is incomplete.

1.5 The Bidder is expected to examine all instructions, forms, terms & conditions and specifications in the Bid Documents. Failure to furnish all information required in the Bid Documents or submission of a Bid not substantially responsive to the Bid Documents in every respect may result in rejection of the Bid. However, the Company’s decision in regard to the responsiveness and rejection of bids shall be final and binding without any obligation, financial or otherwise, on the Company.

1.6 The company reserves the right to split the order among various successful bidders in any manner it chooses without assigning any reason whatsoever.

2. SCOPE OF SUPPLY

Detailed Technical specification/scope of supply is provided in Section-V of this tender document.

3. DISCLAIMER

3.1. This NIT is not an agreement and further it is neither an offer nor an invitation by BRPL to bidders or any other person for award of contract. The purpose of this NIT is to provide bidders information that may be useful to them in the preparation and submission of their bids.

3.2. This Document includes statements, which reflect various assumptions, which may or may not be correct. Each Bidder should conduct its own estimation and analysis and should check the accuracy, reliability and completeness of the information in this Document and obtain independent advice from appropriate sources in their own interest.

3.3. Neither Company nor its employees will have any liability whatsoever to any Bidder or any other person under the law or contract, the principles of restitution or unjust enrichment or otherwise for any loss, expense or damage whatsoever which may arise from or be incurred or suffered in connection with anything contained in this Document, any matter deemed to form part of this Document, provision of Services and any other information supplied by or on behalf of Company or its employees, or otherwise arising in any way from the selection process for the Work.

3.4. Though adequate care has been taken while issuing the Tender document, the Bidder should satisfy itself that Documents are complete in all respects. Intimation of any discrepancy shall be given to this office immediately.

3.5. This Document and the information contained herein are Strictly Confidential and are for the use of only the person(s) to whom it is issued. It may not be copied or distributed by the recipient to third parties (other than in confidence to the recipient's professional advisors).

3.6. It shall be deemed that by submitting a bid, a bidder agrees to release BRPL and its employees, agents and advisors irrevocably unconditionally fully and finally from any and all liability for any claims losses damages costs expenses or liabilities in anyway related to or arising from exercise of any rights and all performance of any obligations under this NIT and or in connection with the bid process to the fullest extent permitted by applicable law and waives any and all rights and all claims it may have in this respect whether actual or contingent whether present or in the future

3.7. BRPL and its employees and advisors also accept no liability of any nature whether resulting from negligence or otherwise arising from reliance of any bidder upon the contents of this NIT. BRPL may in its absolute discretion but without being under any obligation to do so, update amend or supplement the information assessment statement or assumptions contained in this NIT.

3.8. The issue of this tender document does not imply that BRPL is bound to qualify any bidder or to award the contract to any bidder. BRPL reserves the right to reject all or any of the bids without assigning any reasons whatsoever.

4. COST OF BIDDING

The Bidder shall bear all cost associated with the preparation, submission and processing of its Bid and the company will in no case be responsible or liable for the costs.

5. TENDER DOCUMENTS

5.1. The Scope of supply, Bidding Procedures and Contract Terms are described in the Bidding Documents. In addition to the covering letter accompanying Bidding Documents, the Bidding Documents include:

"Check List, Sections, Annexure & Formats as elaborated in CONTENT of this NIT."

5.2. The bidder is expected to examine the tender documents, including all Instructions, Forms, Terms and Specifications. Failure to furnish all information required by the tender documents or submission of a bid not substantially responsive to the tender documents in every respect may result in the rejection of the Bid.

6. AMENDMENT OF TENDER DOCUMENTS

6.1. At any time prior to the deadline for submission of Bids, the Company may for any reason(s), whether at its own initiative or in response to a clarification requested by a prospective Bidder, alter/amend/modify the tender documents by corrigendum /amendment.

6.2. The corrigendum / amendment shall be part of tender document, pursuant to Clause 5.1, and it will be notified

(a) by way of uploading the corrigendum/amendment on BSES website (in case of public tender),

(b) in writing by e-mail to all the Bidders who have received the Bidding Documents by email. (in case of limited tender)

All such corrigendum & amendments will be binding on the bidders.

6.3. In order to provide prospective Bidders a reasonable time in which to take the Amendment into account in preparing their Bids, the Company may, at its discretion, extend the deadline for the submission of Bids.

7. PREPARATION OF BIDS & LANGUAGE

The Bid prepared by the Bidder, and all correspondence, documents etc. relating to the Bid exchanged by the Bidder and the Company shall be written in English Language. Any printed literature furnished by the Bidder may be written in another Language, provided that this literature is accompanied by English translation, in which case, for purposes of interpretation of the Bid. In case of ambiguity in the English translation, interpretation of the Company as regards to translation will be final.

8. DOCUMENTS COMPRISING THE BID

The Bid prepared and submitted by the Bidder shall comprise the following components:

(a) Techno-Commercial Bid & Price Bid as elaborated in RFQ. (STRICTLY AS PER FORMAT)

(b) All the Bids must be accompanied with the required EMD &Tender Fees against each tender.

9. BID FORM

The Bidder shall complete “Original” Bid Form and submit it along with details mentioned in Techno-Commercial bid (without filling price).

10. BID PRICES

10.01 Bidders shall quote for the entire Scope of Supply/Work with a break-up of prices for individual items and Taxes & Duties. The total Bid Price shall also cover all the Supplier's obligations mentioned in or reasonably to be inferred from the Bidding Documents in respect of Design, Supply, Transportation to site, all in accordance with the requirement of Bidding Documents The Bidder shall complete the appropriate Price Schedules included herein, stating the Unit Price for each item & total Price with taxes, duties & freight upto destination.

10.02 The prices offered shall be inclusive of all costs as well as Duties, Taxes and Levies paid or payable during execution of the supply work, breakup of price constituents, should be there.

10.03 Prices quoted by the Bidder shall be **"Firm"** and not subject to any price adjustment during the performance of the Contract. **A Bid submitted with an adjustable price/ Price Variation Clause will be treated as non -responsive and rejected.**

10.04 The qty break-up shown else-where in Price Schedule is tentative. The bidder shall ascertain himself regarding material required for completeness of the entire work. Any item not indicated but is required to complete the job, shall be deemed to be included in the prices quoted.

11. BID CURRENCY

Prices shall be quoted in Indian Rupees Only.

12. PERIOD OF VALIDITY OF BIDS

12.1. Bids shall remain valid & open for acceptance for a period of 120 days from the date of opening of the Bid.

12.2. Notwithstanding above, the Company may solicit the Bidder's consent to an extension of the Period of Bid Validity and the bidder shall be liable to extend the same at the sole cost and consequences of the bidder and no claim from the company in this regard shall be maintainable.

13. ALTERNATIVE BIDS

Bidders shall submit Bids, which comply with the Tender 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 Tender Documents.

14. FORMAT AND SIGNING OF BID

14.1. The original Bid Form and accompanying documents (as specified in Clause 9.0), clearly marked "Original Bid", must be received by the Company at the date, time and place specified in Section-I, RFQ.

14.2. The original copy of the Bid shall be typed or written in indelible ink and shall be signed by the Bidder or a person or persons duly authorized to sign on behalf of the Bidder. Such authorization shall be indicated by written Power-of-Attorney accompanying the Bid. All pages of the bid shall be signed by the signatory accompanied with seal of the Agency.

14.3. The Bid shall contain no interlineations, erasures or overwriting except as necessary to correct errors made by the Bidder, in which case such corrections shall be signed by the person or persons signing the Bid.

15. SEALING AND MARKING OF BIDS

15.1. Bid submission: One original (hard copies) and one duplicate (total two copies) of all the Bid Documents shall be sealed and submitted to the Company before the closing time for submission of the bid.

15.2 The Technical Documents and the EMD shall be enclosed in a sealed envelope and the said envelope shall be super scribed with —"Technical & EMD". The price bid shall be inside another sealed envelope with super scribed "Financial Bid ". Both these envelopes shall be sealed inside another big envelope. All the envelopes should bear the Name and Address of the Bidder and marking for the Original, Copy-1, and the envelopes should be super scribed with —"Tender Notice No. & Due date of opening".

15.2. The Bidder has the option of sending the Bids in person. Bids submitted by Email/Telex/Telegram /Fax will be rejected. No request from any Bidder to the Company to collect the proposals from Courier/Airlines/Cargo Agents etc shall be entertained by the Company.

16. DEADLINE FOR SUBMISSION OF BIDS

16.1. The Original bid must be timely received by the company at the address specified in Section –I, RFQ.

16.2. The Company may, at its discretion extend the deadline for the submission of bids by amending the Tender Documents in accordance with Clause 6.0, in which case all rights and obligations of the Company and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

17. ONE BID PER BIDDER

Each Bidder shall submit only one Bid by itself. A Bidder who submits or participates with more than one Bid will cause all those Bids to be rejected.

18. LATE BIDS

Any Bid received by the Company after the deadline for submission of Bids prescribed by the Company, pursuant to Clause 16.0, will be declared "Late" and rejected and returned unopened to the Bidder.

19. MODIFICATIONS AND WITHDRAWAL OF BIDS

The Bidder is not allowed to modify or withdraw its Bid after the due date of bid submission.

20. EVALUATION OF BID

20.1. The bids will be evaluated techno-commercially on compliance to tender terms and Conditions.

20.2. BRPL reserves the right to ask the bidders to provide any additional information including breakup of the prices as quoted by them against line items.

BSES
RAJDHANI POWER LIMITED

21. CLARIFICATION OF BIDS

To assist in the examination, evaluation and comparison of Bids, the Company may, at its discretion, ask the Bidder for a clarification of its Bid. 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

22. PRELIMINARY EXAMINATION OF BIDS / RESPONSIVENESS

22.1. Company 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.

22.2. 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 Amount will be corrected.

22.3. Company will determine the substantial responsiveness of each Bid to the Tender Documents including execution capability and acceptable quality of the services offered. A substantially responsive Bid is one, which conforms to all the terms and conditions of the Tender Documents without deviation.

22.4. Bid determined as not substantially responsive will be rejected by the Company and may not subsequently be made responsive by the Bidder by correction of the non-conformity.

23. EVALUATION AND COMPARISON OF BIDS

23.1. The evaluation of Bids shall be done based on the delivered cost competitiveness basis.

23.2. The evaluation of the Bids shall be a stage-wise procedure. The following stages are identified for evaluation purposes: In the first stage, the Bids would be subjected to a responsiveness check later on the Techno-Commercial Proposals and the Conditionality of the Bidders would be evaluated.

Subsequently, the Financial Proposals along with Supplementary Financial Proposals, if any, of Bidders with Techno-commercially Acceptable Bids shall be considered for final evaluation.

23.3. The Company's evaluation of a Bid will take into account, in addition to the Bid price, the following factors, in the manner and to the extent indicated in this Clause:

(a) Delivery schedule
(b) Conformance to Qualifying Criteria
(c) Deviations from Tender Documents
(d) Conformity and compliance to the conditions/details provided in pre-bid meeting
(e) Change in the quantity from mentioned in the tender

23.4. The cost of all quantifiable deviations and omissions from the specification, terms and conditions specified in Tender Documents shall be evaluated.

23.5. The Company will make its own assessment of the cost of any deviation for the purpose of ensuring fair comparison of Bids.

23.6. Adjustments in price, if any, based on the above procedures, shall be made for the purposes of comparative evaluation only to arrive at an “Evaluated Bid Price”. Bid Prices quoted by Bidders shall remain unaltered.

24. CONTACTING THE COMPANY

24.1. From the time of Bid opening to the time of contract award, if any Bidder wishes to contact the Company on any matter related to the Bid, it should do so in writing.

24.2. Any effort by a Bidder to influence the Company and/or in the Company‘s decisions in respect of Bid evaluation, Bid comparison or Contract Award, will result in the rejection of the Bidder‘s Bid.

25. COMPANY ’S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS

The Company reserves the right to accept or reject any Bid and to annul the Bidding process and reject all Bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for the Company’s action.

26. AWARD OF CONTRACT

The Company will award the Contract to the successful Bidder whose Bid has been determined to be the lowest-evaluated responsive Bid, provided the Bidder has been determined to be qualified to satisfactorily perform the Contract. Company reserves the right to award order to other bidders in the tender, provided it is required for need of the work.

27. THE COMPANY'S RIGHT TO VARY QUANTITIES

The Company reserves the right to vary the quantity i.e. increase or decrease the Numbers/ quantities without any change in terms and conditions before the award of Contract.

28. LETTER OF INTENT/ NOTIFICATION OF AWARD

The letter of intent/ Notification of Award shall be issued to the successful Bidder whose bids have been considered successful for award of supply/work/order.

The successful Bidder(s) shall be required to furnish acceptance of LOI / notification of award within 7 days of issue of the letter of intent /Notification of Award by Company.

29. CORRUPT OR FRAUDULENT PRACTICES

29.1. The Company requires that the Bidders observe the highest standard of ethics during the entire period of work execution under the Contract. In pursuance of this policy, the Company:

(a) Defines, for the purposes of this provision, the terms set forth below as follows:

"Corrupt practice" means behaviour on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves and/or those close to them, or induce others to do so, by misusing the position in which they are placed, and it includes the offering, giving, receiving, or soliciting of anything of value to influence the action of any such official in the procurement process or in contract execution; and "Fraudulent practice" means a misrepresentation of facts in order to influence a award process or the execution of a contract to the detriment of the Company, and includes collusive practice among Bidders (prior to or after Bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the Company of the benefits of free and open competition.

(b) Will reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question;

(c) Will declare a firm ineligible either indefinitely or for a stated period of time, to be awarded a contract if it at any time determines that the firm has engaged in corrupt or fraudulent practices in competing for, or in executing, a contract.

29.2. Furthermore, It shall be the responsibility of the Bidders to read and understand &aware of the provision stated in the Terms and Conditions of tender before participating in the tender.

30. 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 Company's processing of Bids or award decisions may result in the rejection of the Bidder's Bid.

*****

SECTION III
SPECIAL CONDITIONS OF CONTRACT (SCC)

SECTION III
SPECIAL CONDITIONS OF CONTRACT (SCC)

These Special Conditions of Contract (SCC) shall be read in conjunction with the Terms and Conditions of the Contract, General Conditions of Contract (GCC), Scope of Supply / Work and other documents forming part of the contract wherever the context so requires. Notwithstanding the subdivision of documents into separate sections and volumes, every part of each such document shall be deemed to be supplementary to and complementary of every other part.

1.01 All the Bids shall be prepared and submitted in accordance with these instructions.

1.02 Bidder shall bear all costs associated with the preparation and delivery of its Bid, and the Purchaser will in no case shall be responsible or liable for these costs.

1.03 The Bid should be submitted by the Bidder in whose name the bid document has been issued and under no circumstances it shall be transferred /sold to the other party.

1.04 The Purchaser reserves the right to request for any additional information and also reserves the right to reject the proposal of any Bidder, if in the opinion of the Purchaser, the data in support of RFQ requirement is incomplete.

1.05 The Bidder is expected to examine all instructions, forms, terms & conditions and specifications in the Bid Documents. Failure to furnish all information required in the Bid Documents or submission of a Bid not substantially responsive to the Bid Documents in every respect may result in rejection of the Bid. However, the Purchaser's decision in regard to the responsiveness and rejection of bids shall be final and binding without any obligation, financial or otherwise, on the Purchaser.

2.0 DEFINITION OF TERMS

2.01 "Purchaser/Company" shall mean BSES Rajdhani Power Limited, on whose behalf this bid enquiry is issued by its authorized representative / officers.

2.02 "Bidder" shall mean the firm who quotes against this bid enquiry issued by the Purchaser. "Supplier" or "Supplier" shall mean the successful Bidder and/or Bidders whose bid has been accepted by the Purchaser and on whom the "Letter of Acceptance" is placed by the Purchaser and shall include his heirs, legal representatives, successors and permitted assigns wherever the context so admits.

2.03 "Supply" shall mean the Scope of Contract as described.

2.04 "Specification" shall mean collectively all the terms and stipulations contained in those portions of this bid document known as RFQ, Commercial Terms & Condition, Instructions to Bidders, Technical Specifications and the Amendments, Revisions, Deletions or Additions, as may be made by the Purchaser from time to time.

2.05 "Letter of Acceptance" shall mean the official notice issued by the Purchaser notifying the Supplier that his proposal has been accepted and it shall include amendments thereto, if any, issued by the Purchaser. The "Letter of Acceptance" issued by the

Purchaser shall be binding on the "Supplier" The date of Letter of Acceptance shall be taken as the effective date of the commencement of contract.

2.06 "Month" shall mean the calendar month and "Day" shall mean the calendar day.

2.07 "Codes and Standards" shall mean all the applicable codes and standards as indicated in the Specification.

2.08 "Offer Sheet" shall mean Bidder's firm offer submitted to BRPL in accordance with the specification.

2.09 "Contract" shall mean the "Letter of Acceptance/Purchase Order" issued by the Purchaser/Company.

2.10 "Contract Price" shall mean the price referred to in the "Letter of Acceptance/Purchase Order".

2.11 "Contract Period" shall mean the period during which the "Contract" shall be executed as agreed between the Supplier and the Purchaser in the Contract inclusive of extended contract period for reason beyond the control of the Supplier and/or Purchaser due to force majeure.

2.12 "Acceptance" shall mean and deemed to include one or more of the following as will be stipulated in the specification:

a) The written acceptance of material by the inspector at suppliers works to ship the materials.
b) Acceptance of material at Purchaser site stores after its receipt and due inspection/ testing and release of material acceptance voucher.
c) Where the scope of the contract includes supplying, acceptance shall mean issue of necessary equipment / material takeover receipt after installation & commissioning and final acceptance.

3.0 CONTRACT DOCUMENTS & PRIORITY

3.01 Contract Documents: The terms and conditions of the contract shall consist solely of these RFQ conditions and the offer sheet.

4.0 SCOPE OF SUPPLY -GENERAL

4.01 The "Scope of Supply" shall be on the basis of Bidder's responsibility, completely covering the obligations, responsibility and supplies provided in this Bid enquiry whether implicit or explicit.

4.02 Bidder shall have to quote for the Bill of quantities as listed elsewhere.

4.03 All relevant drawings, data and instruction manuals.

5.0 QUALITY ASSURANCE AND INSPECTION

5.01 Immediately on award of contract, the bidder shall prepare detailed quality assurance plan/test procedure identifying the various stages of manufacture, quality checks performed at each stage, raw material inspection and the Customer hold points. The document shall also furnish details of method of checking, inspection and acceptance standards / values and get the approval of Purchaser before proceeding with manufacturing. However, Purchaser shall have right to review the inspection reports, quality checks and results of suppliers in house inspection department which are not Customer hold points and the supplier shall comply with the remarks made by purchaser or his representative on such reviews with regards to further testing, rectification or rejection, etc. In case of standard items, BRPL shall forward the standard QAP which is to be followed by vendor during manufacturing.

5.02 Witness and Hold points are critical steps in manufacturing, inspection and testing where the supplier is obliged to notify the Purchaser in advance so that it may be witnessed by the Purchaser. Final inspection is a mandatory hold point. The supplier to proceed with the work past a hold point only after clearance by purchaser or a witness waiver letter from BRPL.

5.03 The performance of waiver of QA activity by Purchaser at any stage of manufacturing does not relieve the supplier of any obligation to perform in accordance with and meet all the requirements of the procurement documents and also all the codes & reference documents mentioned in the procurement document nor shall it preclude subsequent rejection by the purchaser.

5.04 On completion of manufacturing the items can only be dispatched after receipt of dispatch instructions issued by the Purchaser.

5.05 All in-house testing and inspection shall be done without any extra cost. The in-house inspection shall be carried out in presence of BSES/BSES authorized third party inspection agency. Cost of Futile/abortive visit(s) shall be debited from the invoices

5.06 Purchaser reserves the right to send any material being supplied to any recognized laboratory for testing, wherever necessary and the cost of testing shall be borne by the Bidder. In case the material is found not in order with the technical requirement / specification, the charges along with any other penalty which may be levied is to be borne by the bidder. To avoid any complaint the supplier is advised to send his representative to the stores to see that the material sent for testing is being sealed in the presence of bidder's representative.

6.0 PACKING, PACKING LIST & MARKING

6.01 **Packing:** Supplier shall pack or shall cause to be packed all Commodities in crates/boxes/drums/containers/cartons and otherwise in such a manner as shall be reasonably suitable for shipment by road or rail to BRPL, Delhi/New Delhi stores/site without undue risk of damage in transit.

6.02 **Packing List:** The contents of each package shall be itemized on a detailed list showing the exact weight, extreme outside dimensions (length, width & weight) of each container/box/drum/carton, Item SAP Code, PO No & date. One copy of the packing list shall be enclosed in each package delivered.

7.01 PRICE BASIS FOR SUPPLY OF MATERIALS

a) Bidder to quote their prices on Landed Cost Basis and separate price for each item. FIRM prices for supply to BRPL Delhi/New Delhi stores inclusive of packing, forwarding, loading at manufacturer's premises, payment of GST.

b) The above supply prices shall also include unloading at BRPL Delhi/New Delhi stores/site.

c) Transit insurance will be arranged by Purchaser; however bidder to furnish required details in advance for arranging the same by Purchaser

8.0 TERMS OF PAYMENT AND BILLING

8.1 Payment shall be made in milestone (MS) as per following:

- **Part A - For Supply**

MS-1: 70% of contact value for of Pricing schedule shall be released subject to fulfillment of following pre-requisites:
(i) Submission of detailed project schedule.
(ii) Submission and approval of detailed engineering documents, Design Documentation for Hardware & Software System, List of Deliverables.
(iii) Delivery and installation of required for hardware and licenses.
(iv) Submission of 10% PBG on part A for warranty period plus three months claim period.

MS-2: 20% of contact value of Pricing schedule shall be released subject to fulfillment of following pre-requisites:
(i) Implementation Closure: which includes integration with sites mentioned in the Scope of the RFP and also integration with the other solutions procured in this RFP, i.e. making the SOC operational UAT, and receiving sign off.
(ii) Closure of all exceptions including Availability of application, Applications tuning completion,
(iii) Approval of Administration & Operator's User's Manual,
(iv) Documentation & training.

MS-3: 10% of contract value for shall be released after 1 month of successful system run without any issues.

- **Part-B - Service (Installation, Commissioning and Testing).**

MS-1: 70% of contract value for shall be released subject to fulfillment of following prerequisites:

(i) Baseline system and application software installation, testing, commissioning, Review and Signoff.
(ii) Installation and Commissioning of all hardware and licences
(iii) System ready for live view, Completion of UAT and Integration Test Reports.

MS-2: 20% of contract value shall be released on completion, i.e.
(i) Closure of all exceptions including Availability of application, Applications tuning completion.
(ii) Approval of Administration & Operator's User's Manual,
(iii) Documentation & training.

MS-3: Balance 10% of contract value for will be released after 1 month of successful system run.

- **Part C- For Operations:**

Payment of Operations service shall be made after the following
a) Post Go-Live Run - Closure of user findings, updated technical doc for changes and tuning as per the scope of work mentioned in section V of system.
b) Submission of 10% PBG for Contract value of Part-C. The validity of BG should be equal to the contract period plus 3 months claim period.
- Quarterly payment of yearly value will be paid at the end of respective quarter on submission of all SLA reports duly certified by Engineer-In-charge.

Note: Milestone payments shall be made in full upon the successful completion of the respective milestone.

Payment terms shall be within 45 days from receipt of invoice supported by BRPL certification of completion of milestone.

8.2 Bidder to submit the following documents against dispatch of each consignment at our Vendor
Support Cell (VSC):
a) Signed copy of accepted Contract (as applicable) & Purchase Order (for first payment)
b) PBG equivalent to 10% of PO Value (including GST) valid till PO validity period, as applicable
c) LR / RR / BL as applicable.
d) Challan as applicable.
e) Two (02) copies of the Supplier's detailed Recipient Invoice showing Commodity description, quantity, unit price, total price and basis of delivery, and is 100% of the value of the consignment claimed.
f) Two (02) copies of Supplier's transporter invoice duly receipted by BRPL Store & Original certificate issued by BRPL confirming receipt of the subject material at Store/Site and acceptance of the same as per the provisions of the contract.
g) Two (02) copies Packing List / Detailed Packing List
h) Approved Test certificates / Quality certificates, if applicable
i) Certificate of Origin, if applicable
j) Material Dispatch Clearance Certificate (MDCC)
k) Warranty / Guarantee Certificate, if applicable
l) Checklist for bill submission.

8.3 Purchaser has the right to recover tax loss, interest and penalty suffered due to any noncompliance of tax laws by the Vendor. In the event, Purchaser is not able to avail of any tax credit due to any shortcoming on the part of the Vendor (which otherwise should have been available to Purchaser in the normal course), then the Vendor at his own cost and effort will get the short coming rectified. If for any reason the same is not possible, then the Vendor will make 'good' the loss suffered by Purchaser due to the tax credit it lost. In such event, any amount paid to the Vendors shall be first attributable to the tax (GST) charged in the invoice and the balance shall be considered towards the 'value' of supply of goods/ services.

8.4 Purchaser shall deduct "Tax Deducted at Source" wherever applicable and at the rate prescribed under the GST Laws or any other Indian law and remit the same to the Government. Necessary TDS certificates as per law shall be issued by the purchase to the vendor.

8.5 Any liability arising out of dispute on the tax rate, classification under HSN, calculation and payment of tax to the Government will be to the Vendor's account.

8.6 Where the supply of Goods is liable to GST under reverse charge mechanism, then the supplier should clearly mention the category under which it has been registered and also that "the liability of payment of GST is on the Recipient of Supply".

9.0 <u>PRICE VALIDITY</u>

9.01 All bids submitted shall remain valid, firm and subject to unconditional acceptance by BRPL Delhi for 120 days from the due date of submission & subsequent corrigendum/amendment/extension of due date of submission. For awarded suppliers/contractors, the prices shall remain valid and firm till contract completion.

10.0 PERFORMANCE GUARANTEE

10.01 Bank guarantee shall be drawn in favour of "BSES Rajdhani Power Ltd" as applicable. The performance Bank guarantee shall be in the format as specified by BRPL.

10.02 Contractor shall submit the performance bank guarantee equivalent to the 10% of the contract value exclusive of GST at the time of claiming the last payment as per clause no. 8.0 (Terms of payment and billing).

11.0 FORFEITURE

11.01 Each Performance Bond established under Clause 10.0 shall contain a statement that it shall be automatically and unconditionally forfeited without recourse and payable against the presentation by BRPL of this Performance Bond, to the relevant bank referred to above, together with a simple statement that supplier has failed to comply with any term or condition set forth in the Contract.

11.02 Each Performance BG established under will be automatically and unconditionally forfeited without recourse if BRPL in its sole discretion determines that supplier has failed to comply with any term or condition set forth in the contract.

12.0 RELEASE

All Performance Bonds will be released without interest within seven (7) days from the last date up to which the Performance Bond has to be kept valid (as defined in Clause 10.0) except for the case set forth in Clause 21.0.

13.0 WARRANTY/DEFECTS LIABILITY PERIOD

13.01 The bidder to guarantee the materials / items supplied against any defect of failure, which arise due to faulty materials, workmanship or design for the entire defects liability period. The proposed system including hardware and software shall have Three (3) year OEM warranty and support, which includes comprehensive maintenance and support of the entire proposed solution. Thereafter the system will be in AMC.

The solution should be proposed along with technical support services as per requirement for Three (3) years from OEM and bidder.
An additional two (2) years warranty and support needs to quote as per price bid .

If during the defects liability period any materials / items are found to be defective, these shall be replaced or rectified by the bidder at his own cost within 30 days from the date of receipt of intimation.

The bidder shall able to depute their service personnel within 48 hours in case of emergency and shall ensure the availability of manpower/spares for the same during warranty period.

14.0 RETURN, REPLACEMENT OR SUBSTITUTION.

BRPL shall give Supplier notice of any defective Commodity promptly after becoming aware thereof. BRPL may in its discretion elect to return defective Commodities to Supplier for replacement, free of charge to BRPL, or may reject such Commodities and purchase the same or similar Commodities from any third party. In the latter case BRPL shall furnish proof to Supplier of the cost of such substitute purchase. In either case, all costs of any replacement, substitution, shipping, labour and other related expenses incurred in connection with the return and replacement or for the substitute purchase of a Commodity hereunder should be for the account of Supplier. BRPL may set off such costs against any amounts payable by BRPL to Supplier. Supplier shall reimburse BRPL for the amount, if any, by which the price of a substitute Commodity exceeds the price for such Commodity as quoted in the Bid.

15.0 EFFECTIVE DATE OF COMMENCEMENT OF CONTRACT:

15.01 The date of the issuance of the Letter of Acceptance/Purchase Order shall be treated as the effective date of the commencement of Contract.

16.0 TIME – THE ESSENCE OF CONTRACT

16.01 The time and the date of completion of the “Supply” as stipulated in the Letter Of Acceptance / Purchase order issued to the Supplier shall be deemed to be the essence of the “Contract”. The Supply has to be completed not later than the aforesaid Schedule and date of completion of supply.

17.0 THE LAWS AND JURISDICTION OF CONTRACT:

17.01 The laws applicable to this Contract shall be the Laws in force in India.

17.02 All disputes arising in connection with the present Contract shall be settled amicably by mutual consultation failing which shall be finally settled as per the rules of Arbitration and Conciliation Act, 1996 at the discretion of Purchaser. The venue of arbitration shall be at New Delhi in India

18.0 EVENTS OF DEFAULT

18.01 Events of Default. Each of the following events or occurrences shall constitute an event of default ("Event of Default") under the Contract:

(a) Supplier fails or refuses to pay any amounts due under the Contract;

(b) Supplier fails or refuses to deliver Commodities conforming to this RFQ/ specifications, or fails to deliver Commodities within the period specified in P.O. or any extension thereof

(c) Supplier becomes insolvent or unable to pay its debts when due, or commits any act of bankruptcy, such as filing any petition in any bankruptcy, winding-up or reorganization proceeding, or acknowledges in writing its insolvency or inability to pay its debts; or the Supplier's creditors file any petition relating to bankruptcy of Supplier;

(d) Supplier otherwise fails or refuses to perform or observe any term or condition of the Contract and such failure is not remediable or, if remediable, continues for a period of 30 days after receipt by the Supplier of notice of such failure from BRPL.

19.0 CONSEQUENCES OF DEFAULT.

(a) If an Event of Default shall occur and be continuing, BRPL may forthwith terminate the Contract by written notice.

(b) In the event of an Event of Default, BRPL may, without prejudice to any other right granted to it by law, or the Contract, take any or all of the following actions;

(i) present for to the relevant bank the Performance Bond;

(ii) Purchase the same or similar Commodities from any third party; and/or

(iii) Recover any losses and/or additional expenses BRPL may incur as a result of Supplier's default

20.0 LIQUIDATED DAMAGES

20.01 If supply of items / equipment is delayed beyond the supply schedule as stipulated in LOI/PO, then the Supplier shall be liable to pay the Purchaser for delay a sum of 1% (One percent) of the basic (ex-works) price for every week of delay or part thereof for individual mile stone deliveries.

20.02 The total amount for delay under the contract will be subject to a maximum of Ten percent (10%) of the total contract value of undelivered units.

20.03 The Purchaser may, without prejudice to any method of recovery, deduct the amount for such damages from any amount due or which may become due to the Supplier or from the Performance Bond or file a claim against the supplier.

21.0 STATUTORY VARIATION IN TAXES AND DUTIES

The total order value shall remain **FIRM** within stipulated delivery period and shall not be adjusted on account of any price increase/variations in commodities & raw materials. However Statutory Taxes, duties and Levies imposed by Competent Authorities by way of fresh notification(s) within the stipulated delivery period shall be borne by BRPL on submission of necessary documents claiming such variation. The variation will be applicable only on such value wherever price breakup of same is submitted by vendor/available in PO/WO

The company reserves the right to review/change the terms & conditions of the Purchase Order/Purchase order prospectively w.e.f. the date of implementation of GST to give effect/take care the impact of GST, if required.

22.0 <u>FORCE MAJEURE</u>

22.01 General

An "Event of Force Majeure" shall mean any event or circumstance not within the reasonable control directly or indirectly, of the Party affected, but only if and to the extent that:

(i) Such event or circumstance materially and adversely affects the ability of the affected Party to perform its obligations under this Contract, and the affected Party has taken all reasonable precautions, due care and reasonable alternative measures in order to prevent or avoid the effect of such event on the affected party's ability to perform its obligations under this Contract and to mitigate the consequences thereof.
(ii) For the avoidance of doubt, if such event or circumstance would not have materially and adversely affected the performance of the affected party had such affected party followed good industry practice, such event or circumstance shall not constitute force majeure.
(iii) Such event is not the direct or indirect result of the failure of such Party to perform any of its obligations under this Contract.
(iv) Such Party has given the other Party prompt notice describing such events, the effect thereof and the actions being taken in order to comply with above clause.

22.02 Specific Events of Force Majeure subject to the provisions of above clause, Events of Force Majeure shall include only the following to the extent that they or their consequences satisfy the above requirements:

(i) The following events and circumstances:
a) Effect of any natural element or other acts of God, including but not limited to storm, flood, earthquake, lightning, cyclone, landslides or other natural disasters.
b) Explosions or fires
(ii) War declared by the Government of India, provided that the ports at Mumbai are declared as a war zone.
(iii) Dangers of navigation, perils of the sea.

22.03 Notice of Events of Force Majeure If a force majeure event prevents a party from performing any obligations under the Contract in part or in full that party shall:

i) Immediately notify the other party in writing of the force majeure events within 7(seven) working days of the occurrence of the force majeure event
ii) Be entitled to suspend performance of the obligation under the Contract which is affected by force majeure event for the duration of the force majeure event.
iii) Use all reasonable efforts to resume full performance of the obligation as soon as practicable
iv) Keep the other party informed of all such efforts to resume full performance of the obligation on a regular basis.
v) Provide prompt notice of the resumption of full performance or obligation to the other party.

22.04 Mitigation of Events of Force Majeure Each Party shall:

(i) Make all reasonable efforts to prevent and reduce to a minimum and mitigate the effect of any delay occasioned by an Event of Force Majeure including recourse to alternate methods of satisfying its obligations under the Contract;

(ii) Use its best efforts to ensure resumption of normal performance after the termination of any Event of Force Majeure and shall perform its obligations to the maximum extent practicable as agreed between the Parties; and

(iii) Keep the other Party informed at regular intervals of the circumstances concerning the event of Force Majeure, with best estimates as to its likely continuation and what measures or contingency planning it is taking to mitigate and or terminate the Event of Force Majeure.

22.05 Burden of Proof In the event that the Parties are unable in good faith to agree that a Force Majeure event has occurred to an affected party, the parties shall resolve their dispute in accordance with the provisions of this Agreement. The burden of proof as to whether or not a force Majeure event has occurred shall be upon the party claiming that the force majeure event has occurred and that it is the affected party.

22.06 Termination for Certain Events of Force Majeure. If any obligation of any Party under the Contract is or is reasonably expected to be delayed or prevented by a Force Majeure event for a continuous period of more than 3 months, the Parties shall promptly discuss in good faith how to proceed with a view to reaching a solution on mutually agreed basis. If a solution on mutually agreed basis cannot be arrived at within a period of 30 days after the expiry of the period of three months, the Contract shall be terminated after the said period of 30 days and neither Party shall be liable to the other for any consequences arising on account of such termination.

22.07 The Purchaser may terminate the contract after giving 7(seven) days notice if any of following occurs:

a) Contractor fails to complete execution of works within the approved schedule of works, terms and conditions
b) In case the contractor commits any Act of Insolvency, or adjudged insolvent
c) Has abandoned the contract
d) Has failed to commence work or has suspended the progress of works
e) Has failed to proceed the works with due diligence and failed to make such due progress

22.08 Limitation of Force Majeure event. The Supplier shall not be relieved of any obligation under the Contract solely because cost of performance is increased, whether as a consequence of adverse economic consequences or otherwise.

22.09 Extension of Contract Period due to Force Majeure event The Contract period may be extended by mutual agreement of Parties by way of an adjustment on account of any period during which an obligation of either Party is suspended due to a Force Majeure event.

22.10 Effect of Events of Force Majeure. Except as otherwise provided herein or may further be agreed between the Parties, either Party shall be excused from performance and neither Party shall be construed to be in default in respect of any obligations hereunder, for so long as failure to perform such obligations shall be due to and event of Force Majeure."

23.0 TRANSFER AND SUB-LETTING

23.01 The Supplier shall not sublet, transfer, assign or otherwise part with the Contract or any part thereof, either directly or indirectly, without prior written permission of the Purchaser.

24.0 RECOVERIES

24.01 When ever under this contract any money is recoverable from and payable by the bidder, the purchaser shall be entitled to recover such sum by appropriating in part or in whole by detecting any sum due to which any time thereafter may become due from the supplier in this or any other contract. Should the sum be not sufficient to cover the full amount recoverable the bidder shall pay to the purchaser on demand the remaining balance.

25.0 WAIVER

25.01 Failure to enforce any condition herein contained shall not operate as a waiver of the condition itself or any subsequent breach thereof.

26.0 INDEMNIFICATION

Notwithstanding contrary to anything contained in this RFQ, Supplier shall at his costs and risks make good any loss or damage to the property of the Purchaser and/or the other Supplier engaged by the Purchaser and/or the employees of the Purchaser and/or employees of the other Supplier engaged by the Purchaser whatsoever arising out of the negligence of the Supplier while performing the obligations under this contract.

27.0 DOCUMENTATION:

The Bidder's shall procure all equipment from BRPL approved sources as per attached specifications. The Bidder's shall submit 5 copies of Material/Type Test Certificates, O&M Manuals, and Approved & As-built drawings. The Bidder's shall ensure for the strict compliance to the specifications and Field Quality Procedures issued by BRPL Engineer in-charge.

28.0 COMMISSIONING SPARES

28.01 Commissioning Spares shall be deemed to be included in the quoted

29.0 DERC GUIDELINES & REGULATIONS

The bidder shall make themselve fully aware & familiarize with prevailing DERC guidelines / regulations.

****

SECTION IV

GENERAL TERMS & CONDITIONS

BSES RAJDHANI POWER LIMITED

SECTION IV

GENERAL TERMS & CONDITIONS

1. DEFINITIONS and INTERPRETATION

The following terms shall have the following meanings:

1.1 "Company": means BSES Rajdhani Power Ltd, a company incorporated under the Companies Act 1956 and having its office at BSES Bhawan, Nehru Place, New Delhi 110 019, which expression shall include its authorized representatives, agents, successors and assigns.
1.2 "Contractor": shall mean the successful Tenderer / vendor to whom the contract has been awarded
1.3 "Rate": The unit rates for the work to be carried out at site shall be as per finalized unit rates through tender. The finalized rates shall be firm for the entire duration of work to be carried out by the Contractor under the Purchase order and are not subject to escalation for any reason whatsoever.
1.4. CONTRACT SPECIFICATION: The terms "CONTRACT Specification" shall mean the Technical specification of the work as agreed by you and description of work as detailed in Annexure-I enclosed herewith and all such particulars mentioned directly/referred to or implied as such in the contract.
1.5 SITE: The terms "Site" shall mean the working location in BRPL area. Under this tender, working location shall be as mentioned elsewhere.
1.6 ENGINEER IN CHARGE: "Engineer In-charge" means the Company's authorized representative for the purpose of carrying out the work.

2. EXAMINATION OF SITE AND LOCAL CONDITIONS:

The contractor is deemed to have visited the site of the work and ascertained therefore all site conditions and information pertaining to his work. The company shall not accept any claim whatsoever arising out of the difficult site/terrain/local conditions, if any.

3. LANGUAGE AND MEASUREMENT:

The CONTRACT issued to the contractor by the company and all correspondence and documents relating to the CONTRACT placed on the Contractor shall be written in English language.

Metric System shall be followed for all dimension, units etc.

4. RATES:

The rates finalized for this order shall be firm for the entire duration of work carried out by the Contractor under the order and are not subject to any variation and escalation for any reason whatsoever.

The cost of insurance during loading/unloading of materials/ equipments during its storage and handling/erection at site for installation is included in the contractor's scope and value is included in the unit rates finalized.
The unit rates finalized are also inclusive of barricading and watch & ward during execution and no separate charges shall be paid for the same.

The cost of training of BRPL Official shall be included in the prices quoted by vendor.

5. TAXES AND DUTIES:

Prices are inclusive of all taxes and duties and GST. However, IT as per applicable rate will be deducted from your bills as Tax Deduction at Source (TDS).The order involves only services and labour hence WCT/VAT not applicable to the order.

The total order value shall remain **FIRM** within stipulated delivery period and shall not be adjusted on account of any price increase/variations in labour. However Statutory Taxes, duties and Levies imposed by Competent Authorities by way of fresh notification(s) within the stipulated delivery period shall be borne by BRPL on submission of necessary documents claiming such variation. The variation will be applicable only on such value wherever price breakup of same is submitted by vendor/available in PO/WO.

6. DEFECT LIABILITY PERIOD:

The bidder to guarantee the materials / items supplied against any defect of failure, which arise due to faulty materials, workmanship or design for the entire defects liability period. The proposed system including hardware and software shall have Three (3) year OEM warranty and support, which includes comprehensive maintenance and support of the entire proposed solution. Thereafter the system will be in AMC.

The solution should be proposed along with technical support services as per requirement for Three (3) years from OEM and bidder. An additional two (2) years warranty and support needs to quote as per price bid .

If during the defects liability period any materials / items are found to be defective, these shall be replaced or rectified by the bidder at his own cost within 30 days from the date of receipt of intimation.

The bidder shall able to depute their service personnel within 48 hours in case of emergency and shall ensure the availability of manpower/spares for the same during warranty period.

7. PERFORMANCE GUARANTEE

7.01 Bank guarantee shall be drawn in favour of “BSES Rajdhani Power Ltd” as applicable. The Performance Bank guarantee shall be in the format as specified by BRPL.

7.02 Contractor shall submit the performance bank guarantee equivalent to the 10% of the order value exclusive of GST at the time of claiming the last payment as per clause no. 8.0 (Terms of payment and billing , Section II).

8. SUB-CONTRACTING / SUBLETTING:

Bidder shall not assign or transfer the whole or any part of this Purchase order or any other benefits accruing there from nor shall it subcontract / sublet the whole or any part of the Works without the prior written consent of COMPANY.

In the event the contractor assigns this Purchase order, contractor's assignees shall be bound by the terms and conditions of this Purchase order and shall , if deemed necessary by COMPANY at the time of such assignment, undertake in writing to be so bound by this Purchase order.

Notwithstanding the subletting / subcontracting of any portion of the works, contractor shall remain wholly responsible for the carrying out, completion and satisfactory execution of Works in all respects in accordance with this Purchase order, specification, approved drawings and data sheets.

9. <u>INDEMNITY:</u>

Contractor shall indemnify and save harmless COMPANY against and from any and all liabilities, claims, damages, losses or expenses arising due to or resulting from:

a) any breach non-observance or non-performance by contractor or its employees or agents of any of the provisions of this Purchase Order.
b) any act or omission of contractor or its employees or agents.
c) any negligence or breach of duty on the part of contractor, its employees or agents including any wrongful use by it or them of any property or goods belonging to or by COMPANY.

Contractor shall at all times indemnify COMPANY against all liabilities to other persons, including he employees or agents of COMPANY or contractor for bodily injury, damage to property or other loss which may arise out of or in consequence of the execution or completion of Works and against all costs charges and expenses that may be occasioned to COMPANY by the claims of such person.

10. <u>EVENTS OF DEFAULTS</u>:

COMPANY may, without prejudice to any of its other rights or remedies under the Purchase Order or in law, terminate the whole or any part of this Purchase Order by giving written notice to the Contractor, if in the opinion of COMPANY, contractor has neglected to proceed with the works with due diligence or commits a breach of any of the provisions of this Purchase order including but not limited to any of the following cases:

a) Failing to complete execution of work within the terms specified in this Purchase order.
b) Failing to complete works in accordance with the approved schedule of works.
c) Failing to meet requirements of specifications, drawings, and designs as approved by COMPANY.
d) Failing to comply with any reasonable instructions or orders issued by COMPANY in connection with the works.
e) Failing to comply with any of the terms or conditions of this Purchase order.

In the event COMPANY terminates this Purchase order, in whole or in part, on the occurrence of any event of default, COMPANY reserves the right to engage any other subcontractor or agency to complete the work or any part thereof, and in addition to any other right COMPANY may have under this Purchase order or in law including without limitation the right to penalize for delay under clause 15.0 of this Purchase order, the contractor shall be liable to COMPANY for any additional costs that may be incurred by COMPANY for the execution of the Work.

11. RISK & COST:

If the Contractor of fails to supply as per specification / as per the direction of Engineer's In-charge within the scheduled period and even after the extended period, the contract shall got cancel and company reserves the right to get the supply executed from any other source at the Risk & Cost of the Contractor. The Extra Expenditure so incurred shall be debited to the Contractor.

12. ARBITRATION:

To the best of their ability, the parties hereto shall endeavor to resolve amicably between themselves all disputes arising in connection with this LOA. If the same remain unresolved within thirty (30) days of the matter being raised by either party, either party may refer the dispute for settlement by arbitration. The arbitration to be undertaken by two arbitrators, one each to be appointed by either party. The arbitrators appointed by both the parties shall mutually nominate a person to act as presiding arbitrator before entering upon the reference in the event of a difference between the two arbitrators and the award of the said presiding arbitrator in such a contingency shall be conducted in accordance with this provisions of the Indian Arbitration & Conciliation Act, 1996 and the venue of such arbitration shall be in the city of New Delhi only.

13. FORCE MAJEURE:

13.1 General:

An “Event of Force Majeure” shall mean any event or circumstance not within the reasonable control, of the Party affected, but only if and to the extent that:

(i) Such event or circumstance, despite the exercise of reasonable diligence, could not have been prevented, avoided or reasonably foreseen by such Party;

(ii) Such event or circumstance materially and adversely affects the ability of the affected Party to perform its obligations under this Contract, and the affected Party has taken all reasonable precautions, due care and reasonable alternative measures in order to prevent or avoid the effect of such event on the affected parties ability to perform its obligations under this Contract and to mitigate the consequences thereof. For the avoidance of doubt, if such event or circumstance would not have materially and adversely affected the performance of the affected party had such affected party followed good industry practice, such event or circumstance shall not constitute force majeure.

(iii) Such event is not the direct or indirect result of the failure of such Party to perform any of its obligations under this Contract; and

(iv) Such Party has given the other Party prompt notice describing such events, the effect thereof and the actions being taken in order to comply with above clause

13.2 Specific Events of Force Majeure:

Subject to the provisions of above clause, Events of Force Majeure shall include only the following to the extent that they or their consequences satisfy the above requirements:
The following events and circumstances:

(i) Effect of any natural element or other acts of God, including but not limited to storm, flood, earthquake, lightning, cyclone, landslides or other natural disasters, and

(ii) Explosions or fires

(iii) Declaration of the Site as war zone.

Any order, regulation, directive, requirement from any Governmental, legislative, executive or judicial authority.

13.3 Notice of Events of Force Majeure

If a force majeure event prevents a party from performing any obligations under the Contract in part or in full, that party shall :

(i) Immediately notify the other party in writing of the force majeure events within 2 working days of the occurrence of the force majeure event

(ii) Be entitled to suspend performance of the obligation under the Contract which is affected by force majeure event for the duration of the force majeure event
(iii) Use all reasonable efforts to resume full performance of the obligation as soon as practicable

(iv) Keep the other party informed of all such efforts to resume full performance of the obligation on a regular basis

(v) Provide prompt notice of the resumption of full performance or obligation to the other party.

13.4 Mitigation of events of force majeure:

The Contractor shall:

(i) Make all reasonable efforts to prevent and reduce to a minimum and mitigate the effect of any delay occasioned by an Event of Force Majeure, including applying other ways in which to perform the Contract;

(ii) Use its best efforts to ensure resumption of normal performance after the termination of any Event of Force Majeure and shall perform its obligations to the maximum extent practicable as agreed between the Parties; and Keep the Company informed at regular intervals of the circumstances concerning the event of Force Majeure, with best estimates as to its likely continuation and what measures or contingency planning it is taking to mitigate and or terminate the Event of Force Majeure.

13.5 Burden of proof:

In the event that the Parties are unable in good faith to agree that a Force Majeure event has occurred to an affected party, the parties shall resolve their dispute in accordance with the provisions of this Contract. The burden of proof as to whether or not a force majeure event has occurred shall be upon the party claiming that the force majeure event has occurred and that it is the affected party.

13.6 Terminations for certain events of force majeure:

If any obligation of any Party under the Contract is or is reasonably expected to be delayed or prevented by a Force Majeure event for a continuous period of more than 1 (one) month during the Term of the Contract the Contract shall be terminated at the discretion of the Company and neither Party shall be liable to the other for any consequences arising on account of such termination.

14. SECRECY CLAUSE:

The technical information, drawing and other related documents forming part of Purchase order and the information obtained during the course of investigation under this Purchase order shall be the Company's executive property and shall not be used for any other purpose except for the execution of the Purchase order. The technical information drawing, records and other document shall not be copied, transferred, or divulged and/ or disclosed to third party in full/part, not misused in any form whatsoever except to the extent for the execution of this Purchase order.

These technical information, drawing and other related documents shall be returned to the Company with all approved copies and duplicates including drawing/plans as are prepared by the Contractor during the executions of this Purchase order, if any, immediately after they have been used for agreed purpose.
In the event of any breach of this provision, the contractor shall indemnify the Company against any loss, cost or damage or claim by any party in respect of such breach.

15. TERMINATION:

"During the course of the execution, if at any time BSES observe and form an opinion that the work under the order is not being performed in accordance with the terms of this Agreement, BSES reserves its right to cancel this Agreement giving 30 days notice mentioning the reason for the termination of the agreement and BSES will recover all damages including losses occurred due to loss of time from Contractor.

16. QUALITY:

Contractor shall ensure that strict quality is maintained and execution of works under this Purchase order and Works are executed in conformity with the Specification.

All tools, tackles, instruments and other equipments used in the execution of the Works shall be duly calibrated as required and Contractor shall maintain proper records of such tools, tackles, instruments and / or equipment.

17. ACCEPTANCE

Acceptance of this Purchase order implies and includes acceptance of all terms and conditions enumerated in this Purchase order in the technical specification and drawings made available to you consisting of general conditions, detailed scope of work, detailed technical specification & detailed equipment, drawing. Complete scope of work and the Contractor's and Company's contractual obligation are strictly limited to the terms set out in the Purchase order. No

amendments to the concluded Purchase order shall be binding unless agreed to in writing for such amendment by both the parties.
However, during the course of the execution of the Purchase order, if at any time the Company's representative observe and form an opinion that the work under the Purchase order is not being performed in accordance with the terms of this Purchase order, the company reserves its right to cancel this Purchase order forthwith without assigning any reason and the Company will recover all damages including losses occurred due to loss of time from the Contractor.
We request you to please sign the duplicate copy of this Purchase order as a token of your acceptance and return to us.

18. TERMINATION

1.1. TERMINATION BY COMPANY FOR NON PERFORMANCE

During the course of the execution, if at any time the Company observe and forms an opinion that the work under the order is not being performed satisfactory and the performance of the Contractor not found satisfactory, the Company reserves its right to cancel/ terminate this Agreement giving minimum 30 days' notice without assigning any reason and the Company will recover all damages including losses occurred due to loss of time from the Contractor. After termination of the agreement, the Contractor shall immediately stop all activities related to the work terminated. This is without prejudice to other rights under the terms of contract. The Contractor shall hand over the Company all drawing/documents prepared for this contract up to the date of cancellation of order.

1.2. PREMATURE TERMINATION

The order can be terminated by the Company before the expiry of its term under the following conditions:

(i) The Contractor repudiates this order or otherwise evidences intention not to be bound by this order;
(ii) The Contractor assigns, mortgages, or charges or purports to assign, mortgage, or charge any of its obligations or rights in contravention to the provisions of this order; or, transfers or negates any of its obligations in contravention to the provisions of this order.
(iii) The Contractor breaches the Secrecy/Non-disclosure Clause/Confidentiality obligations.
(iv) If at any stage during the tenure of the work order, Contractor is found to be involved or indulging or even attempting illegal, unlawful action or activities or some fraudulent or even trying to take or ask bribe from any customer or to give bribe official/staff or misuse or abuse any meter or property of the Company.
(v) The Company shall be entitled to deduct from any money due or to becomes due to the Contractor, money paid or payable by way of compensation as aforesaid or cost or expenses in connection with any claims thereto. The Contractor shall abide by the decision of the Company as to the amount payable by the Contractor under the provision of this clause.

1.3. TERMINATION BY COMPANY FOR CONVENIENCE

The Company shall, in addition to any other right enabling it to terminate the Contract, have the right to terminate the Contract at any time without assigning any reason, by giving a written notice of minimum 30 days to the Contractor. The Contract shall stand terminated on the date as per the notice but such termination shall be without prejudice to the rights of the Parties accrued on and before the date of termination.

****

SECTION V

SCOPE AND TECHNICAL SPECIFICATIONS

SCOPE AND TECHNICAL SPECIFICATIONS

1.0 Company Profile

BRPL Rajdhani Power Ltd (BRPL) is the leading utility company having presence across the entire value chain of power businesses i.e. distribution of power. BRPL is India's largest private power distribution company, serving over ~2.56 million consumers with 24 x 7 uninterrupted, reliable and quality power spread over 750 sq. km with a customer density of ~3407 per sq km in 22 districts across South and West areas.

Request for Procurement (RFP) is invited suitably experienced parties to build and operate Security Operations Center (SoC) including supply and commission of technologies SIEM(Security Incident and Event Management), SOAR(Security Orchestration Automation and Response),UEBA (User and Entity Behavior Analytics), NBAD (Network Behavior Anomaly Detection), Threat Intelligence, Threat Hunting, Incident Management along with operations of Security Operation Center. Supply, Installation and commissioning for SoC solution with Three (03) years warranty, support and operations for BSES RAJDHANI POWER LTD (BRPL)

1.1. BRPL intended to setup SoC center including technologies SIEM, SOAR, UEBA, NDR/NBAD, Threat hunting, Threat Intelligence, Incident Management.
1.2. The proposed solution should be sized for 10,000 sustained EPS in BRPL.
1.3. The UEBA solution license should be for 4500 users for BRPL.
1.4. The proposed solution should be provided along with licenses for 10,000 sustained EPS at correlation layer but should be able to handle 1:2 peak EPS at correlation layer without dropping events or queuing events (for SIEM) from the 1st day.
1.5. SOAR should be sized with unlimited playbooks and with Three (3) concurrent user licenses supplied along with the solution.
1.6. The next gen SIEM platform should be capable to provide automatic notification to SOC teams as defined in playbooks based on Conditional decision & Trigger Functions.
1.7. The proposed next gen SIEM solution should have the capability to compress the logs by at least 50% for storage optimization.
1.8. Proposed next gen SIEM should have ability to detect MITRE ATT&CK techniques for IT and OT.
1.9. Proposed next gen SIEM should have advance analytics features like Real-Time Threat Detection and Management, Behavioral Analytics and Treat Hunting. Threat Intelligence with MITRE, MISP.
1.10. Proposed next gen SIEM should be based on Open architecture with greater interoperability
1.11. Proposed next gen SIEM should have advance machine learning and other AI-based techniques to cut down detection time for malicious activity.
1.12. The proposed solution must support 1000+ data sources with predefined parsing/normalizations rules out of the box.
1.13. SSL Descriptor should be consider by the bidder if required for NDAB/NDR
1.14. The Platform must include log management, NG SIEM, Host Forensics, UEBA, NDR, File Integrity Monitoring, Security Analytics, Big Data Analytics, Security Automation and

Orchestration engine (includes but not limited to Incident Management, Incident Response), Advanced Correlation within the same platform with no additional 3rd party solution)

1.15. The solution should have a common event database in the security big data lake.

1.16. The solution must provide Metrics and reports on mean time to detect (MTTD) and mean time to respond (MTTR) as KPI for team performance

1.17. The platform must provide predictive Threat Intelligence Using Behavior Modeling

1.18. The proposed solution built-in FIM (File Integrity Monitoring) must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data

1.19. The proposed solution must support the 1000+ out-of-the-box analytics rules and use cases not limited UEBA – NDR – MITRE – Power sector, IT Ops – Compliance from day one.

1.20. Next gen SIEM solution should be EPS based and must support logs from unlimited devices or sources

1.21. The next gen SIEM solution should support high availability features and should be proposed in HA mode for all layers at DC

1.22. No Events should be dropped during Spikes, even if license limits gets exceeded: The proposed solution must not, under any circumstances, drop incoming events.

1.23. Bidder to integrate next gen SIEM solution with various BRPL IT system and OT security solution for log collection. The responsibility for integration of SIEM with various applications and solutions lies with the Bidder. BRPL shall provide adequate support to the Bidder for the purpose of integration throughout the contract period.

1.24. SoC should support, understand and correlated events of IT and OT systems both.

1.25. Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based, Risk based etc.

1.26. Provide system landscape design along with server, storage. Server and storage sizing should be done keeping 20000 EPS and raw log retention for atleast 6 months. Appropriate Hardware (server/storage) required should be provided by the bidder along with all required licenses.

1.27. Solution should be appliance/hardened device based and appliance should able to support 20000 EPS without any upgrades from day 1.

1.28. Hardware and software to be sized by the OEM as bundle with maximum performance guarantee in HA mode. Hardware appliance should be tuned and engineered for the SIEM & SOAR system. OEM should own overall performance responsibility of the system.

1.29. Offered system to have MIS reporting feature with dashboards integrated with email and SMS

1.30. Provide solution document covering SIEM, SOAR, UEBA, NDR and SOC operations

1.31. The solution should have capability of integrating all devices irrespective of their Hardware/OS/application/Database in BRPL environment. Further, in case of any upgradation of current Hardware/OS/Database/application in BRPL, the same should be integrated with next gen SIEM solution within one month. No extra cost will be payable to bidder for any customization and integration.

1.32. Bidder should provide and implement all feature upgrades or version upgrades during contract period without any cost.

1.33. There should be Maker Checker feature available in case any configuration/policy change is being done by any user

1.34. The proposed SoC solution must be extensible and scalable to accommodate the BRPL's growing needs and keep up with complex operational requirements.

1.35. Bidder should provide support to plug out any vulnerability found in the SoC technology solutions as and when identified by BRPL as well as by the OEM. Patches made available by the OEM should be applied immediately. All vulnerabilities should be closed immediately or within 15 days of reporting the same to bidder

1.36. The successful bidder, in coordination with the OEM must make a detailed study of BRPL infrastructure and requirements relating to the solution, prepare a detailed plan document/road map mentioning all the pre-requisites, timeframe of milestones/achievements within the Completion Period leading to the full operationalization of the solution. The bidder will provide a detailed low-level Solution design document and Project Plan. The implementation would start only after sign-off of the documents submitted by bidder/Go-ahead from the BRPL.

1.37. Successful bidder will require signing Non-Disclosure Agreement, as per format provided by BRPL before start of project.

1.38. Bidders require to provide the POC as per the BRPL request and requirement before finalization of the system. BRPL reserve the rights to qualify or disqualify bidder solution based on PoC out come and deliverables. BRPL may request to visit the bidder's SOC site to ascertain capabilities. Bidder shall facilitate such visits at their client site or SOC center.

1.39. Custom parser development required during implementation and operations phase will be in bidder's scope.

1.40. Bidder should involve OEM as part of SoC deployment (OEM should be equally responsible and involved in all stages viz architecture design, implementation, governance, training etc). Technical training (admin and user) should be arranged from OEM for BRPL resources by bidder.

1.41. Proposed OEM should have TAC Support center based in India and bidder should consider TAC support from OEM during the contract period for any support required from OEM.

RAJDHANI POWER LIMITED

Scope of Work - OPERATIONS

2.1. SCOPE OF WORK

BRPL wishes to outsource its Operations of Security Operation Centre to a partner with rich experience in handling and running SOC through multi-location presence.

a) The Bidder shall be responsible for 24*7*365 management of all security alarms, alerts and incidents.

b) Bidder needs to provide independent SOC operations for BRPL and needs to be run from company locations for L1 and L2 support. L3 support needs to be provided from bidder location. A dedicated shared L3 resource needs to be provided to BRPL. In case if L3 resource is required to visit BRPL site for any incident handling same needs to be arranged onsite by bidder with no additional cost to BRPL.

c) Bidder shall define dedicated support window for BRPL SOC operations with team of Security manager, Analyst, and Engineers at BSES premise.

d) Bidder should help BRPL to mitigate any security incidents during contract period

e) Bidder should have well qualified and experienced security professionals on their rolls with required skill sets and certifications like CEH, CISSP, CISA, CISM, OSCP, CCSP, CompTIA security+ etc.

f) Bidder should deploy certified professionals / resources on site on offered SIEM in BRPL SOC. If resources are not certified bidder should ensure their certification within 3 months after deployment at BRPL site.

g) Bidder should configure different dashboards as per BRPL requirements

h) Bidder needs to adhere guidelines and regulations issued by CERT-In, CEA or NCIIPC during full contract period w.r.t cyber security, incident reporting, SOC operations for nation critical sectors.

i) Bidder should evaluate BRPL ticketing system to log tickets of SOC and if found existing ticketing system to be incapable then access to bidder ticketing system to be provided to BRPL for tracking purpose and SLA calculations.

j) Bidder should integrate offered SIEM/SOAR/UEBA/NDR solution to existing or bidder ticketing system for incident case logging.

k) Bidder should provide real-time incident alert and tracking from ticketing system to BRPL nominated persons via email/SMS or Whatsapp.

l) Bidder should provide with program manager as SPOC for all purposes.

m) Bidder should be MSSP having SOC 2, Type II certified. Certified report – 1st page of report to be submitted.

n) Bidder should have knowledge/ experience of IT and OT-ICS domains (Optional).

BRPL will provide the access of security devices like WAF, SIEM and SOAR etc installed at BRPL premise and bidder needs to monitor and manage its operations.

A security operations center (SOC) is a centralized unit that deals with security issues on an organizational and technical level. It comprises the three building blocks for managing and enhancing an organization's security posture: people, processes, and technology.

Thereby, governance and compliance provide a framework, tying together these building blocks.

An information security operations center (ISOC) is a dedicated site where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

1) Security analysts are cybersecurity first responders. They report on cyber threats and implement any changes needed to protect the organization. They're considered the last line of defense against cybersecurity threats, work alongside security managers and cybersecurity engineers, and will report to the CISO.
2) Security engineers are in charge of maintaining and updating tools and systems. They are also responsible for any documentation that other team members might need, such as digital security protocols.
3) The SOC manager is responsible for the SOC team. They direct SOC operations and are responsible for syncing between analysts and engineers; hiring; training; and creating and executing on cybersecurity strategy. They also direct and orchestrate the company's response to major security threats.
4) Incident response (IR) is responsible for managing incidents as they occur, and communicating security requirements to the organization in the case of a significant data breach.

Management and operation of the SOC including (but not limited to) the following processes:

- SoC monitoring
- Incident detection, response and handling
- Threat intel and analytics
- SoC use case management
- Capacity management
- Problem management
- Release management
- Quality assurance
- Incident triaging and Escalation management processes
- Configuration and Change Management
- Breach response and investigations
- Daily standard security operating procedures
- Training procedures, playbooks and material
- Reporting metrics and continuous improvement procedures
- Data retention and disposal procedures
- Playbook creation in SOAR
- Ticketing system for SIEM/SOAR incidents

Selected bidder needs to sign NDA with BRPL before start of its services and comply with the BRPL's security policy.

2.2. TEAM STRUCTURE

Job description of team structure is indicative and is not limited to:

Job Profile	Job Description	No. of Shifts	Service duration
SOC Operator (L1 level)	• Incident detection • 24*7 monitoring of incidents and raise alerts • Incident reporting and escalation • Report creation • Security patch advisories • System health monitoring Note: In case of any incident detection during off hours wherein L2 & L3 resources required for further investigation. Bidder should ensure to arrange required set of resources for further investigation in spite of service duration and no. of shift.	3	24x7x365
SOC Analyst (L2 level)	• SIEM and SOAR product administration • Incident validation • Detailed analysis of attacks and incident response • Solution recommendation for issues • Manage security devices • Risk analysis for change management for security devices • Escalation point for device issue resolution • Resolve escalation • Identified missed incidents • Maintain knowledge base • Defining security breaches • Follow-up with the concerned departments/vendor on the remediation steps taken • Resolve queries from BRPL stakeholders • Coordinate and be present to discuss with BRPL stakeholders in person	2	12x6x365
SOC Manager	The technical team leader will be responsible for: • Troubleshooting technical problems for the successful execution of project. • Implementing changes to meet BRPL's demands and specification. • Providing direction, instructions and guidance to the team for achieving a certain goal. • Proffered to have knowledge/ experience of IT and OT-ICS systems • Developing and implementing a timeline their team will use to reach its end goal. • Track incident detection and closure • Present regular metrics and reports • Identify new alerts requirement	1	8x6

2.3. HIGH LEVEL DELIVERABLES

Areas	Activities	Deliverables

Security Event Monitoring and Response	Log Monitoring; Server Monitoring; Security and Network Device monitoring	• 24*7*365 log monitoring
		• Detection of threats from integrated log sources and based on the use cases defined
		• Event Analysis
		• Alerts as per defined escalation matrix
		• Real-time alerts for priority tickets on email and SMS
		• High Criticality Security alert (Priority 1):
		  ○ Response: 30 minutes
		  ○ Resolution: 1 hour
		• Medium Criticality Security alert (Priority 2):
		  ○ Response: 2 hours
		  ○ Resolution: 6 hours
		• Low Criticality Security alert(Priority 3):
		  ○ Response: 6 hours
		  ○ Resolution: 24 hours
		• Logs of any duration of one year as asked by BRPL: within 24 hours
		• New use case creation as suggested by BRPL : within 3 working days

Network Threat Hunting	Analytics Based Hunting & IOC Based Hunting	• Once in 24 hours • Notification of alerts generated through analytical models on Threat Hunting enabling hunting for attacks including but not limited to Lateral Movement, Malware Beaconing, Data Exfiltration, Watering Hole, Targeted network attacks, Dynamic DNS attacks etc.
Incident Management	Incident Analysis, Identification of all components of the incident, root cause analysis and mitigation plans	• Major incident process for P1 & P2 incidents • Provide logs and incident report for any identified security incident. • Coordinate with BRPL's Team and help to contain attack/incident. • Provide evidences for legal and regulatory purpose in the form of log data.
SOC Maturity Improvement	SOC report on analysis and insights from data	• Quarterly briefings on Analysis and insights from data: trends, high risks areas, roadmap for strategic improvements, security posture benchmarking. Briefings on global threat trends, regulatory trends and cyber technology trends.
Report Management	Periodic reports; Trends analysis. Customized and ad-hoc reports,	Following are the minimum reports, bidders shall provide to BRPL:

		• Daily reports: ○ Top attacker, attacks and attack targets, trends report ○ Top firewall ports access report (inbound/outbound) ○ Top signature triggered ○ Top account brute forced ○ Top systems infected ○ Top virus infection in the network ○ SIEM/monitoring tool performance report • Weekly reports: ○ Weekly security incidents status report ○ Daily device utilization report ○ Device availability report ○ Device: Incident, service request and change status report ○ Weekly threat advisory and vulnerability report ○ Top signature triggered ○ Top account brute forced ○ Top systems infected ○ Top virus infection in the network • Monthly reports: ○ Executive summary report for all the services ○ Monthly Security incident status report ○ Monthly security incident trend analysis ○ Monthly device availability report ○ Monthly risk report • Quarterly reports: ○ Quarterly Security incident status report ○ Quarterly security incident trend analysis ○ Quarterly cyber security activities report
Global Intelligence Feeds	Continuous and regular global feeds from external known agencies.	• Threat & Vulnerability advisories in form of E-mails on need basis or at least once in a week • Monthly report on recommendations for security improvements. • Quarterly report on Historical, Operational, Analytical and predictive Analysis.

2.4. MEASURE OF PERFORMANCE:

BRPL will measure the performance of SOC teams to continuously improve their processes. Here are a few important metrics that can help demonstrate the scale of activity in the SOC, and how effectively analysts are handling the workload.

Metric	Definition	What it Measures
Mean Time to Detection (MTTD)	Average time the SOC takes to detect an incident	How effective the SOC is at processing important alerts and identifying real incidents
Mean Time to Resolution (MTTR)	Average time that transpires before the SOC takes action and neutralizes the threat	How effective the SOC is at gathering relevant data, coordinating a response, and taking action
Total cases per month	Number of security incidents detected and processed by the SOC	How busy the security environment is and the scale of action the SOC is managing
Types of cases	Number of incidents by type: web attack, attrition (brute force and destruction), email, loss or theft of equipment, etc.	The main types of activity managed by the SOC, and where preventative security measures should be focused
Analyst productivity	Number of units processed per analyst — alerts for Tier 1, incidents for Tier 2, threats discovered for Tier 3	How effective analysts are at covering maximum possible alerts and threats
Case escalation breakdown	Number of events that enter the SIEM, alerts reported, suspected incidents, confirmed incidents, escalated incidents	The effective capacity of the SOC at each level and the workload expected for different analyst groups

2.5. SERVICE LEVELS & THRESHOLDS

Service levels provide for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. Bidder shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the bidder shall be reviewed by BRPL on quarterly basis and BRPL shall:

- Check performance of the bidder against defined service levels over the review period of 3 month and consider any key issues of the past period’s performance statistics including major incidents, service trends, etc.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

In case, if desired, BRPL may initiate an interim review to check the performance and the obligations of the Agency. The BRPL will conduct quarterly review of the services rendered by the Service Provider at mutually agreed schedules, dates and representatives from both the BRPL & BRPL and Service Provider should attend such performance review meetings. The Service Levels may be reviewed periodically i.e. quarterly and revised, if required.

The service levels shall take into consideration the following aspects-

- Equipment Availability Related Service Levels
- Technical Support desk Services
- Compliance and Reporting Procedures
- Quality and Availability of Required Staff

The following measurements and targets shall be used to track and report performance on a regular basis. The targets shown in the following table are applicable for the duration of the contract:

<table>
<tr><th>S. No.</th><th>Service Area</th><th>Service Level</th><th>Penalty</th></tr>
<tr>
<td>1</td>
<td>Monitoring & Incident Alerting</td>
<td>1. Log Analysis Services
2. 24x7 monitoring of all in-scope devices.
3. Categorization of Incidents into High, Medium and Low priority shall be carried out in consultation with the selected bidder during the contract period.
4. All High and Medium priority incident should be logged as incident tickets and alerted as per SL.
• High Criticality security alerts within 30 minutes of the event identification.
• Medium priority security alerts within 2 hours of the event identification.
• Low priority security alerts within 6 hours of the event identification

Note: All incidents to be reported as per CERT-In, CEA or NCIIPC guidelines.</td>
<td>1. High Criticality Security Alerts (Priority 1) to be reported within 30 minutes and resolved within 1 hour
2. Medium Criticality Security Alerts (Priority 2) to be responded within 2 hours and resolved within 6 hours
3. Low Criticality Security Alerts (Priority 3) to be responded within 6 hours and resolved within 24 hours
4. SLs pertaining to new use cases, request of logs, new devices integrations will also be used in below table calculations

<table>
<tr><td>SL compliance measured/month</td><td>Penalty</td></tr>
<tr><td>97.5% and above</td><td>N.A.</td></tr>
<tr><td>95% to 97.49%</td><td>1% of quarterly payment</td></tr>
<tr><td>92.5% to 94.99%</td><td>3 % of quarterly payment</td></tr>
<tr><td>90% to 92.49%</td><td>5 % of quarterly payment</td></tr>
<tr><td><90%</td><td>10 % of quarterly payment</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td>2</td>
<td>Incident Investigation Reports and Closure</td>
<td>Sending out detailed investigation report post alert notification. Action plan/mitigation steps should be personnel as per the below SL:
• High Criticality incident within 1 hour of the event identification.
• High priority incident within 4 hours of the event identification.
• Medium priority incident within 12 hours of the event identification

Note: All incidents to be reported as per CERT-In, CEA or NCIIPC guidelines.</td>
<td>1. High priority incident within 1 hours
2. Medium priority incident within 6 hours
3. Low priority incident within 24 hours

<table>
<tr><td>SL compliance measured/month</td><td>Penalty</td></tr>
<tr><td>97.5% and above</td><td>N.A.</td></tr>
<tr><td>95% to 97.49%</td><td>1% of quarterly payment</td></tr>
<tr><td>92.5% to 94.99%</td><td>3% of quarterly payment</td></tr>
<tr><td>90% to 92.49%</td><td>5% of quarterly payment</td></tr>
<tr><td><90%</td><td>10% of quarterly payment</td></tr>
</table>
</td>
</tr>
<tr>
<td>3</td>
<td>Reports and Dashboard</td>
<td>1. Daily Reports: By 10:00 AM everyday
2. Weekly Reports: By 10:00 AM, Monday
3. Monthly Reports: 5th working day of each month</td>
<td>Threshold: SL compliance 95%, measured per quarter
Penalty: 3% of quarterly payment.</td>
</tr>
<tr>
<td>4</td>
<td>Quality of Resource and Availability</td>
<td>1. Number and quality of resources at minimum as defined in Section 3.2 & 3.1
2. Not more than one replacement every quarter
3. No replacements called for by the BRPL & BRPL on account of misconduct or performance of any resource</td>
<td>No Default in all 3 parameters- No Penalty
Default in any or all of the parameter- 5% of quarterly billing.</td>
</tr>
</table>

**** SL may be changed by the BRPL at its discretion during signing of agreement with the qualified bidder.***

Maximum penalty in a quarter will be capped to 10% of quarterly SOC operation charges. Bidder shall not be responsible for SL impact where the delay is not attributable to the bidder. All such cases have to be adequately evidenced.

3.0 DOCUMENTATION & TRAINING

3.1. The bidder shall provide the required Documentation specified in the document for all the proposed equipment and systems.

3.2. The documentations shall include but not limited to the followings: -

3.2.1. User guides for those who shall be using the system

3.2.2. Operational guides for administrators and technical support officers;

3.2.3. Installation, configuration, fine-tuning and maintenance guides;

3.2.4. Configuration documentations, which includes the various parameter settings in the various system after the fine-tuning processes.

3.2.5. System Flows and Description in the respect of functional and operational requirements.

3.2.6. General and technical information of the individual equipment;

3.2.7. Inventory documents of the entire proposed equipment

3.3. Technical hands-on training for Administrator and Operational teams of BRPL & BRPL by trainer from OEM. Training premises can be finalize at the time of training

4.0 COMMISSIONING AND ACCEPTANCE TEST:

4.1. The bidder shall submit full documentation and status report on the commissioning and handover to BRPL & BRPL.

4.2. The bidder shall propose, design, implement and perform Commission and Acceptance test plan with the BRPL & BRPL.

4.2.1. Bidder shall prepare criteria for commissioning and acceptance for the various systems in consultation and approval of BRPL & BRPL.

4.2.2. The criteria shall be vetted and approved by BRPL & BRPL.

4.3. The criteria shall be attached as appendix with the commissioning and acceptance documents.

5.0 STATUTORY & CYBER SECURITY COMPLIANCE:

- To comply with the requirement of the Ministry of Power, the Bidder has to provide artifacts/certificates against the below points along with or before delivery of material/invoice.
- All software components are tested in the country, to check for any kind of embedded malware/Trojan/cyber threat and for adherence to Indian Standards.

i. All such testing has been done in certified laboratories designated by the Ministry of Power (MoP).

ii. Any import of equipment components/parts from "prior reference" countries as specified or by persons owned by, controlled by, or subject to the jurisdiction or the directions of these "prior reference" countries will have required prior permission of the Government of India (If the components have not been imported from such prios reference countries, please mention so clearly in the certificate, in which case next point does not apply).

iii. Where the equipment components/parts are imported from "prior reference" countries, with special permission, the protocol for testing in certified and designated laboratories has been approved by the Ministry of Power (MoP).

Ref: Order of Ministry of Power, Govt. of India vide Order no. No.25- 11/6/2018-PG dated 2nd July, 2020.

- It has been mentioned in order directions 1 & 2 that all equipment, components, and parts imported for use in the Power Supply System and Network shall be tested in the country to check for any kind of embedded malware/ trojan /cyber threat and for adherence to Indian Standards. Also all such mentioned testing are to be carried out in certified laboratories that will be designated by the Ministry of Power (MoP).

- This order shall apply to any item imported for end use or to be used as a component, or as a part in manufacturing, assembling of any equipment or to be used in power supply system or any activity directly or indirectly related to power supply system. For equipment/component/part, which are imported from “prior reference” countries, there are specific directions provided in the order.
- In continuation of this order, the certified laboratories for cybersecurity conformance testing are notified via MoP order No. 12/34/2020-T&R dated 8th June 2021.

Ref: Order of Ministry of Power, Govt. of India vide Order no. No.12/34/2020-T&R dated 8th June, 2021

- The equipment’s supplied as IT/communication products shall have valid certificate of common criteria as per ISO/IEC15408 issued by signatories of Common Criteria Recognition Agreement (CCRA). In case product sourcing is from prior reference countries the certificate for common criteria shall have to be obtained from government laboratories in India according to IC3S scheme by MEIT, which is signatory of CCRA.
- MoP Order no. No.25- 11/6/2018-PG dated 2nd July, 2020)

6.0. WARRANTY & SUPPORT

6.1. Offered solution should be with OEM warranty and support

6.2. The proposed system including hardware and software shall have Three (3) year OEM warranty and support, which includes comprehensive maintenance and support of the entire proposed solution. Thereafter the system will be in AMC.

6.3. The solution should be proposed along with technical support services as per requirement for Three (3) years from OEM and bidder.
An additional two (2) years warranty and support needs to quote as per price bid .

6.4. The proposed solution should have life of minimum 7 years from the date of supply. The OEM must support the same for next 7 years however if any product including hardware and software which is declared end of life product by OEM during the support period of system, in this case the tenderer should supply replaced model or next higher model/version of the Product on Free of cost basis. Bidder shall provide OEM certificate of the same.

6.5. During warranty period the software must be covered with necessary minor or major upgrades (Software support and upgrade-Major i.e. Version and minor too)

6.6. Warranty/ Support should be 2hrs response, 7 days/week, 24 hours/day.

6.7. System design should be with 99.8% availability annually. OEM to vet the design and provide the confirmation on system availability as totality.

6.8. Support should cover quarterly Preventive Maintenance Service / health checkup of the system

6.9. A single point contact for all maintenance calls shall be established. Routine preventive maintenance shall be scheduled and performed at least four times for one calendar year.

6.10. System warranty will be started after installation, commissioning and Go-live of SIEM Solution. Timeline will be six months or go-live whichever is earlier.

6.11. SOC Operations will start after go-live and successful run of one month of SIEM/SOAR solution.

7.0 GUARANTEED TECHNICAL PARTICULARS

Technical bid should comprise of pointwise compliance/deviation sheet against each clause mentioned in this specification. In event of deviation, logic for the same and details of alternate offer shall be clearly given.

8.0 PROJECT TIME-LINE:

Project completion duration will be 6 months from the date of release of order.

5 Annexure: MoP Order no. No.25- 11/6/2018-PG dated 2nd July, 2020)

No.25-11/6/2018-PG
Government of India
Ministry of Power
Shram Shakti Bhawan, Rafi Marg, New Delhi – 110001
Tele Fax: 011-23730264
*****

Dated 02/07/2020

ORDER

Power Supply System is a sensitive and critical infrastructure that supports not only our **national defence, vital emergency services** including health, disaster response, **critical national infrastructure** including classified data & communication services, defence installations and manufacturing establishments, logistics services but also the **entire economy** and the **day-to-day life** of the citizens of the country. Any danger or threat to Power Supply System can have catastrophic effects and has the potential to cripple the entire country. Therefore, the Power Sector is a **strategic and critical sector.**

The vulnerabilities in the Power Supply System & Network mainly arise out of the possibilities of cyber attacks through malware / Trojans etc. embedded in imported equipment. Hence, **to protect the security, integrity and reliability of the strategically important and critical Power Supply System & Network** in the country, the following directions are hereby issued :-

(1) All equipment, components, and parts imported for use in the Power Supply System and Network shall be tested in the country to check for any kind of embedded malware/trojans/cyber threat and for adherence to Indian Standards.

(2) All such testings shall be done in certified laboratories that will be designated by the Ministry of Power (MoP).

(3) Any import of equipment/components/parts from "prior reference" countries as specified or by persons owned by, controlled by, or subject to the jurisdiction or the directions of these "prior reference" countries will require prior permission of the Government of India

(4) Where the equipment/components/parts are imported from "prior reference" countries, with special permission, the protocol for testing in certified and designated laboratories shall be approved by the Ministry of Power (MoP).

This order shall apply to any item imported for end use or to be used as a component, or as a part in manufacturing, assembling of any equipment or to be used in power supply system or any activity directly or indirectly related to power supply system.

This issues with the approval of Hon'ble Minister of State for Power and New & Renewable Energy (Independent Charge).

(Goutam Ghosh)
Director
Tel: 011-23716674

To:

No.12/34/2020-T&R
Government of India / Bharat Sarkar
Ministry of Power / Vidyut Mantralaya
(T&R Division)
** ** **

"F" Wing, 2nd Floor, Nirman Bhawan
New Delhi, dated 8th June, 2021.

ORDER

Subject: Testing power system equipment for use in the Supply System and Network in the country for Cyber Security - Regarding

Reference is invited to this Ministry's Order No.25-17/6/2018-PG dated 2nd July, 2020 on the above subject. Central Power Research Institute (CPRI) is hereby notified as the nodal agency for testing power system equipment for cyber security.

2. Further the designated laboratories and the products for which cyber security conformance testing is to be undertaken on payment of applicable test charges are given in Annexure – 1.

3. The protocols to be followed for testing the products for cyber security conformance testing, testing criteria and details of type tests are given in Annexures – 2, 3 & 4 respectively.

4. The subject order will be reviewed and updated as needed and the same will be notified as and when any changes / updates are implemented.

5. This issues with the approval of the competent authority.

Encl: As above.

(Ujjwal Kumar Sinha)
Deputy Secretary to Govt. of India
Tel: 23063497

To:

BSES
RAJDHANI POWER LIMITED

Technical Specification

Security Information and Event Management (SIEM) will be used to capture, correlate, monitor and alert all the incoming data to BRPL from different source of IT and OT. The tool will be receiving log data as well as data packets from different sources and must have the capability to ingest and correlate both log data as well as flow data. Tool must meet the objective of BRPL to detect any anomalous behavior by analyzing the incoming traffic. Below table states the features of a SIEM tool as cited by BRPL , however, the features are not restricted to the below mentioned list, but the tool is required to have the below mentioned features:

S. No.	Specification	Compliance Yes/No	Remarks
	General Requirement		
1	SoC solution must be dedicated on premise solution and support IT and OT		
2	The solution must support automated identification and classification for type of assets (i.e. servers, network devices, mail servers, data base servers etc.,)		
3	The solution must provide the ability to encrypt communications on the network between SIEM components and SIEM		
4	The solution must ensure all distributed system components continue to operate when few parts of the NG-SOC solution fails or loses connectivity (i.e. management engine goes off-line all separate collectors continue to capture logs).		
5	The solution can be software based with hardened OS or big data- based platform or equivalent technology. Clearly elaborate the components constituting SIEM, SOAR, UEBA, NDR. Mention in detail associated infrastructure expected from Data Centre for effective functioning of SoC.		
6	High-Level Diagram to be submitted for SoC solution ensuring no data loss and optimal bandwidth utilization in WAN and LAN.		
7	The solution should demonstrate ‘ease of use’. Ease of use is critical to the successful deployment and on- going use of the solution		
8	The solution should allow a wizard-based interface for rule creation. The solution should support logical operations and nested rules for creation of complex rules		
9	Collection, Co-relation and Console layer should be physically and logical separate.		

10	The solution should support log collection, correlation and alerts for the number of devices mentioned in scope.		
	Log Management		
11	Raw and normalized Logs should be handled and stored in tamper proof way across SIEM solution. Any alter/modify tamper rights w.r.t Raw logs should be captured in audit logs.		
12	The solution must provide a complete audit trail and accountability during the incident handling for forensic investigations. The system should have ability to perform event forensics to determine what really happened before, during, and after the event.		
13	The solution should be customizable to accept and process unknown log formats.		
14	The solution must provide capabilities for time stamping, efficient storage and compression (minimum 50%) of collected data.		
15	The solution must support/normalize event time stamps across multiple time zones.		
16	The system should provide the ability to write a custom parser or filter for an unknown new event and a new log		
17	The solution shall allow bandwidth management, rate limiting, at the log collector level.		
18	Left Blank		
19	Log Search Interface: The proposed solution must provide a simple, intuitive search interface using following search methodologies: a) Search Drilldown b) Search Patterns c) Search Operators d) Regular Expression e) Flow-based Searches f) Search Criteria g) Search Time Range h) Search Results View i) Search Export j) Search Combinations		
20	The solution must have an automated backup/archival/ recovery process.		
21	The solution must provide near-real-time analysis of events. Mention lag, if any, between the actual event and its reporting with analysis		

22	The solution should provide the ability to aggregate and analyze events based on a user specified filter. Give the list of in-built filters (IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.) available. Also explain the ease of use of filters.		
23	Universal Log Analysis: The proposed solution must contain system content that can be used for cyber-security, compliance, application and IT & OT operations monitoring and must support additional content specific to regulations like ISO27001, IT-Act etc..		
24	Log Management Performance: The proposed solution should have event handling capacity with low capacity incremental blocks.		
25	Log Data Integrity: The proposed solution must provide audit quality integrity and alerting mechanisms in case of any access/change.		
26	Search Performance – Structured Data: The proposed solution search performance must be capable of searching through millions of structured (indexed) events		
27	Search Performance – Unstructured Data: The proposed solution search performance must be capable of searching through millions of unstructured (raw) log messages		
28	Saved Search Filters: The proposed solution must provide a simple, intuitive way of allowing users to save search filters for later use and to be shared with other authorized users.		
29	Historical Analysis: The proposed solution must be capable of processing and storing large volumes of historical log data that can be restored and analyzed for forensic investigation purposes.		
30	Remote File System: Remote File System: The proposed solution must provide a web interface/CLI for mapping to remote file systems using NFS or CIFS to backup log data or read raw log files into the system. The solution must provide a capability to forward logs to external systems without any dependence on OEM specific formats/tools		
31	Retention Policies: The proposed solution must provide the ability to define multiple retention policies based on time periods, storage allocation, device type, governance, etc.		
32	Retention Enforcement: The proposed solution must enforce data retention policies automatically without necessitating manual data disposition or clean –up efforts.		
33	Retention Policy Suspension: The proposed solution must provide the ability to suspend the retention policy manually and allow administrators to increase the retention period dynamically for the purpose of evidence preservation in the event of pending litigation.		

34	The solution should be capable of integrating with vulnerability management solutions, aiding in the detection of patches, and providing comprehensive reporting.		
	Event & Log Collection		
35	The proposed Solution must provide the following capabilities: **a**. Incident review framework to facilitate incident tracking, investigation, pivoting and closure. **b**. Threat intelligence framework that automatically collect, aggregate indicators of compromise from threat feeds		
36	Solution should support the collection application log data from custom / in-house developed web applications, with or without explicit custom parser development.		
37	The solution should provide time based and forward feature at each log collection point.		
38	The proposed Solution must be able to provide the capability to annotate events, modify status, and build a chronological timeline for the incident before and after a triggered event.		
39	The solution should be able to collect and process raw logs in real- time from any IP Device including Networking devices (router/switches/voice gateways), Security devices (IDS/IPS, AV, Patch Mgmt, Firewall/DB Security solutions), Operating systems (Windows (all flavors), Unix, LINUX (all flavors), AIX etc), Mainframe(z/196), Virtualization platforms, Databases (Oracle, SQL, DB2 etc.), Storage systems, and Enterprise Management systems etc. The list of supported systems with which SIEM can INTEGRATE in each category viz. Network, Security, OS, Databases, Servers, Mainframe, Anti-malware system, Storage, Backup system.		
40	The solution should be able to conduct agent less collection of logs except for those which cannot publish native audit logs		
41	The system should support, not restricted to, the following log and event collection methods: ▪ Syslog – UDP (as detailed in RFC 3164) and TCP (as detailed in RFC 3195). ▪ Flat file logs such as from DNS, DHCP, Mail servers, web servers etc. ▪ Windows events logs – Agent-based or agent- less. ▪ FTP, S/FTP, SNMP, ODBC, CP-LEA, SDEE, WMI, JDBC,		
42	Distributed Event Processing: The proposed solution must collect logs in a distributed manner, offloading the processing requirements of the log management system for tasks such as filtering, aggregation, compression and encryption.		

43	Custom Collection API: The proposed solution must have a software tool to allow customers to create integration with unsupported legacy or internally developed event sources. The software tool must allow customers to integrate with Syslog, log files, databases etc. and support the ability to parse multi -line log files.		
44	Categorized Event Data: The proposed solution must categorize log data into an easy-to-understand humanly-readable format that does not require knowledge of OEM-specific event IDs to conduct investigation, define new correlation rules, and/or create new reports/dashboards.		
45	Secure Transport: The proposed solution must provide encrypted transmission of log data from device to SIEM system.		
46	Reliable Transport: Log Transmission should use reliable TCP protocol that will ensure retransmission in the event of protocol failure to ensure that no log data is lost in transit.		
47	Collection Health Monitoring: Any failures of the event collection infrastructure must be detected immediately and operations personnel must be notified via various communication mediums such as e -mail, ticket etc. Health monitoring must include the ability to validate that original event sources are still sending events.		
48	Event Filtering: The proposed solution must provide inline options to reduce event data at the source by filtering out unnecessary event data.		
49	Event Aggregation: Aggregation must be flexible in which normalized fields can be aggregated and provide the ability to aggregate in batches or time windows.		
50	Caching & Batching: The proposed solution must support local caching and batching at collection level in case of connectivity failures.		
51	Compression: Proposed solution should allow compression to conserve bandwidth.		
52	Raw Event Data: proposed solution must support the option of collecting raw event data using Syslog, FTP, SCP, SNMP protocols, and any other protocol required for collection of logs etc. This ensures original audit quality data is available for forensics.		
53	Windows Event Logs: The proposed solution must be able to integrate with a Windows Domain in an agent-less fashion and collect the event logs from multiple systems without requiring any agents to be installed on the end devices.		
54	Time Correction: The proposed solution must be capable of collecting event time for systems along with collection time and alerting time. This allows integrity for forensic analysis to determine the original time of the event source and what the system time was for each system component processing the event.		

BSES
RAJDHANI POWER LIMITED

55	Centralized Management: The proposed solution must be managed centrally to configure all features, backup configurations and push software updates etc. using one centralized interface.		
56	The solution should have native geo-location feature.		
57	The solution proposed should collect and analyse audit trails logs and Netflow information (all types of logs – ODBC, SDEE, Syslog, Checkpoint etc.) to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach in the scoped environment.		
58	SIEM should have the ability to integrate/leverage technologies like Apache's Kafka and/or NiFi for data collection and enrichment.		
59	Support for operational technology (OT) and Internet of Things (IoT) technologies and environments (e.g., ICS/SCADA)		
60	The EPS burst should be processed in real time without dropping or queuing to ensure real time analysis of threat.		
61	A template for each application should be made consisting of format of log and type (IIS, https, transaction log, login/logout audit log for each application etc..), future applications (NOAR etc..) should be able to send log data to SIEM through log collection APIs.		
Correlation			
62	Correlation Rules: The proposed solution must provide many correlations rules out-of-the-box to automate the incident detection and workflow process.		
63	Cross-Device Correlation: The proposed solution must be capable of correlating activity across multiple devices out-of-the-box to detect authentication failures, perimeter security, worm outbreaks and operational events in real -time without the need to specify particular device types		
64	The solution should have intelligence to minimize false positives alerts, correlate and deliver accurate alerts.		
65	The solution must support the ability to correlate against vulnerability assessment tool.		
66	The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in five minutes then generate an alert.		
67	The solution must support correlated incidents for applications, databases, servers, networks etc. based on feed from other solutions like PAM, WAF, VAPT, NBAD, TIP, Threat hunting Centre and UEBA		

68	The solution must provide many correlations rules out-of-the-box. Again, option of creating/configuring new rules must be available. Please provide the complete list/count of rules which are available out of the box from the system		
69	Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: 1) Vulnerability based 2) Statistical based 3) Historical based 4) Heuristics based 5) Behaviour based on source entity, applications etc. 6) Information Leak 7) Unauthorized Access 8) Denial of Service 9) Service Unavailable 10) Phishing attack 11) Pattern based rules 12) Profiling		
70	Solution should support at least rule based, non-rule based, vulnerability based and statistical based correlation.		
71	The solution should have out-of-box rules for popular IDS, firewalls, antivirus, operating systems, etc. Documentation of the correlation rules should also be provided.		
72	The solution should have intelligence to extract Information from leading global intelligence sources, proposed threat intelligence platform and use it for valid correlation.		
73	The solution should be able to collect and store configuration data from various devices and use it for analysis.		
74	The system should provide the capability for correlate and identify zero-day threats on the network.		
75	The system should have ability to perform multiple event correlation to process all time and transaction- based events to provide actionable data and incident awareness.		
76	The system should provide real-time as well as historical correlation of events. This includes the techniques used for correlation of different events across different monitored devices. Describe the process for handling both real-time events and historical events.		

77	The system should provide adequate categorization and prioritization of the collected and aggregated events from the monitored log sources. This entails a deep understanding of the event types and criticality associated with the events for the supported log sources. The categorization may by be HIGH, MEDIUM, LOW or color coding		
78	The system/solution should have the ability to correlate all the fields in a log.		
79	The solution must leverage both Supervised / Un-supervised Machine learning techniques without signatures		
80	Events should not be dropped if its exceeding the EPS limitation. Events should not be dropped even if log consolidation/log correlation layer goes down for the period of 48 hours		
81	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, vulnerability data, etc.		
82	Future Proofing: The proposed solution must provide a level of confidence that reporting will continue to work and not have to be modified if a particular technology, such as a Firewall or IDS product, is replaced with a newer product or OEM. The reports should continue to run and include the new technology into the report criteria automatically.		
83	Ad hoc Report Performance: The proposed solution must have a mechanism to collect meta-data used by reports that track information over long periods of time so that running these reports ad hoc does not take considerably longer than any other reports.		
84	Custom Dashboards: The proposed solution must provide the framework to create custom visual displays for any business group using user provided images and backgrounds to support security operations, business workflow, risk management and branding use cases.		
85	Dashboard Drill-Down: The proposed solution must provide the ability to allow analysts to drill -down from graphical dashboards to the underlying event data.		
86	Content Management: The proposed solution must provide the ability to synchronize its resource contents (i.e. rules, dashboards, reports, filters etc) automatically across multiple instances of the product, to support multi-instance/high-event-rate deployments		
87	Statistical Correlation: The proposed solution must be capable of keeping a statistical baseline of "normal" monitored activity. This includes attacker, target, ports, protocols and session data.		

BSES
RAJDHANI POWER LIMITED

88	Correlation Flexibility: solution must be capable of running cross device correlation, real time correlation, and historical correlation at the same time.		
89	Historical Correlation: The proposed solution must be capable of monitoring attack history against critical asset or by particular users.		
90	Session Correlation: The proposed solution must provide the ability to correlate DHCP, VPN and Active Directory events to provide session tracking for every user in the enterprise. This is essential for pinpointing who was using a particular workstation historically during an incident investigation.		
91	Dynamic / Static Lists: The proposed solution must allow users to define either whitelist or blacklists that can be used as inclusion or exemption during the correlation process. Additionally, the correlation engine should utilize dynamic lists to provide important information such as shared user monitoring, session tracking, attack history and privileged system access. Product must support import capability to create/ update monitoring list which can be dynamically add/ remove values without manual intervention		
92	Correlation Performance: The proposed solution must be capable of efficiently presenting categorized data to the correlation engine to allow real -time detection and response.		
93	Rule Chains: The system must provide the ability to allow rules to be triggered in a series, matching various correlation activity before an alert is generated.		
94	Alert Thresholds: The proposed solution must provide the ability to aggregate and suppress alerting with granular options and use conditional logic to determine if an alert should be generated.		
95	Re-Usable Content: The solution must allow users to create objects such as filters or search queries that are reusable throughout the system		
96	Content Editor: The proposed solution must provide a common interface to create or modify resources within the system. All aspects of this editor must apply to the development of rules, reports, dashboards and any other resource that will be created in the system.		
97	Integration Command: The proposed solution must provide integration commands that can execute a local or remote script for tools to assist administrators and/or analysts. Tools such as nslookup, ping, traceroute, port info, web search and who is should be available and preconfigured in the console to access on the local machine		

Alerting			
98	The solution must provide real time alerting based on observed security threats. The critical alerts should be transmitted using multiple protocols and mechanisms such as email, SMS, voice call etc. based on agreed policies.		
99	Solution must be capable of monitoring attack/incident history against critical assets or by particular users.		
100	The solution should have option to assign priority against the alerts to allow prioritization based on multiple configurable characteristics such as asset type, protocol, application, etc.		
101	Left Blank		
102	Real-Time Alerts: The proposed solution must be capable of generating alerts based on filter pattern matches for operational health monitoring		
103	Threshold Alerts: In addition to real -time alerts, the system must provide historical, threshold alerts, configured from saved search queries.		
104	Alert Filters: The proposed solution must provide pre - defined alerts and provide the ability to re-use pre-defined filters and own created filters as alert criteria		
105	Alert Delivery: The proposed solution must provide options of how alerts are delivered to operations or security personnel. At a minimum the options must include reporting to the web console, send an email, generate an SNMP trap to an external management system, and send alert on mobiles. The solution must be capable of doing all these concurrently for each alert		
106	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, vulnerability data, etc		
Reporting			
107	The centralized web based/console user interface should drill down on reports and incident alerts on real time basis with full filtering capabilities		

108	The solution must provide reporting engine for out-of- box reports, customized reports, ability to schedule reports, compliance reports, historical trend reports with the following options: 1. Detailed reports of non-compliant activities and policy violations in the network. 2. Historical system-based, user-based and network-based event data for compliance auditing. 3. Information about threat response and mitigation measures carried out to prevent attacks. 4. The solution must provide reporting engine for out-of-box reports, customized reports, ability to schedule reports, compliance reports, historical trend reports etc. 5. The solution should provide out of box templates for reports on ISO, PCI, SOX and other standards. 6. The solution must support direct drill-down from the UI. 7. The system should allow scheduling reports. 8. Reports should be available in pdf and csv format.		
109	The solution should allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities		
110	The reports generated should be possible to be formatted as a complete document e.g. custom header, footer, sections and content.		
111	Reports should be possible to be scheduled and mailed across to the requisite person.		
112	All out of box content should be made available for use as and when published by the OEM		
113	The solution should provide out of box templates for reports on ISO 27001 standards at no additional cost.		
114	Pre-Defined Reports: The proposed solution must provide pre- defined, out-of-the-box reports for Operations, Security and Compliance that can easily be modified.		
115	Compliance Reports: Solution should provide compliance auditing, alerting and reporting for governances for ISO 27001.		
116	Customized Reports: The proposed solution must provide the ability for customers to create their own reports with report templates, reporting wizard as well as an advanced interface for power users to create their own custom report queries.		

117	Report Export: The proposed solution reporting function must be capable of exporting reports in various formats. At a minimum, the report formats should be, excel, csv, Adobe Acrobat (.pdf) etc. The reporting function should also allow the reports to be run and viewed ad - hoc by user as well.		
118	Report Scheduling: The proposed solution must provide the ability for customers to schedule and email reports to run hourly, daily, weekly or monthly as an attachment. There must be numerous output formats and delivery options for scheduled reports.		
119	Run-Time Report Options: The proposed solution reporting engine must provide the ability to filter, highlight, and modify various report functions at runtime. This should include the ability to selectively define which device group or storage partition to report upon		
120	The solution should provide an integrated case management system which should ensure independent investigation eliminating the risk of possible intervention of administrator.		
	Dashboard		
121	The SIEM solution must provide central management of all components and administrative functions from a single web based / console user interface. It must have out of the box ready algorithm from day one..		
122	The centralized dashboard to monitor the alerts and events from all devices of Data Centre at its locations and from the tools provided as a part of NG-SOC solution.		
123	The solution should provide customizable management console/dashboard which can be provided to different Teams. Access to the solution should be restricted based on role of that team/user, which should be configurable.		
124	The solution dashboard should be in the form of a unified portal that can show correlated alerts/ events from multiple disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases, etc.		
125	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users.		
126	The dashboard should show the status of all the tools deployed as part of the SOC, including availability, bandwidth consumed, system resources consumed (including database usage)		

BSES
RAJDHANI POWER LIMITED

127	It should be possible to categorize events while archiving for example, events for network devices, antivirus, servers etc.		
128	Customizable Dashboards: The proposed solution should provide dashboards specific to each user and should be user configurable. The dashboards must be capable of displaying multiple daily reports specific to each users job function.		
129	Solution should provide Dashboard not limited to Audit Dashboard, Security Dashboard, Risk Dashboard, Analytics Dashboard, Asset Dashboard, User Activity Monitoring dashboard, User/ Identity Dashboard, Threat Intelligence Dashboard, Etc.		
130	Solution should provide Pre-built Dashboards using auto-configuring of thresholds and baselines.		
131	Solution should have dashboards to identify and investigate security incidents, reveal insights in your events, accelerate incident investigations, monitor the status of various security domains, and audit the incident investigations.		
132	Solution should help to investigate incidents with specific types of intelligence. a. Threat intelligence dashboards use the threat intelligence sources and custom sources that you configure to provide context to your security incidents and identify known malicious actors in your environment. b. User intelligence dashboards allow you to investigate and monitor the activity of users and assets in your environment. c. Web intelligence dashboards help you analyse web traffic in your network and identify notable HTTP categories, user agents, new domains, and long URLs		
133	Dashboard Integration: The proposed solution must be accessed through web interface so that display dashboards, queries and reports can be executed and viewed.		
134	The dashboard should drill down on events and find the IP addresses and geo-locations from the sources of suspicious or malicious IPs.		
135	SIEM solution should be able to map correlation rules/use cases with MITRE tactics and techniques to get better visibility of incidents and shall be a part of the proposed solution.		

136	Integration Command: The proposed solution must provide integration commands that can execute a local or remote script for tools to assist administrators and/or analysts. Tools such as nslookup, ping, traceroute, port info, web search and whois should be available and preconfigured in the console to access on the local machine		
137	The solution must normalize common event fields (i.e. usernames, IP addresses, hostnames, and log source device etc.) from disparate devices across a multi- Bidder network. Solution to provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields.		
138	The solution must support information collected from File Integrity / Activity Monitoring (FIM / FAM) Security software and tools.		
139	The system should be able to support integration with proposed threat hunting Centre and other Security Analytics tools		
140	Solution should integrate with IDS, IPS, Firewall etc to consume alert data and based on that perform investigative and remediation actions.		
141	Left Blank		
142	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.		
143	Alerting: The proposed solution should provide the ability to integrate with enterprise-class network management systems through SNMP.		
144	Syslog Forwarding: The proposed solution must be able to receive raw (i.e. unprocessed) event data in the form of syslog messages or text log files, in addition to receive the raw original event data from collectors.		
145	Solution should have an OOTB bidirectional integration with Threat Intel Platform.		
146	The system should receive feeds from a threat intelligence repository maintained by the OEM which consists of inputs from various threat sources and security devices across the globe		
147	The system should be capable to consume Threat Intelligence from Third Party sources as well.		
	Administration		
148	The Solution should provide web/ thick based administration user interface for device management and monitoring.		

BSES
RAJDHANI POWER LIMITED

149	The system should support Network Time Protocol for time synchronization.		
150	The solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service.		
151	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.		
152	There should be an automated switch over to secondary collector in case of failure on the primary collector. No performance degradation is permissible even in case of collector failure.		
153	SIEM Solution should have common interface/native integration with NDR, UEBA/UBA, SOAR solution.		
154	The monitoring capabilities to ensure that the proposed system is functioning under optimal parameters e.g. CPU/storage etc.		
155	Administrative Interface: The proposed solution must provide a Web / thick client interface used for administrative tasks including but not limited to configuration, updates, patches, backups, restores, content creation, analysis, user management and all other tasks.		
156	Administration Dashboard: The proposed solution must provide a single administrative dashboard to analyze the system load, event flow and storage performance trends.		
157	No Database Administrator: The proposed solution must not require a Database Administrator to perform implementation, tuning or other DB administrative tasks.		
158	Simple System Backup: The proposed solution must provide a simple method for automatically and manually backing up and restoring system configuration data.		
159	Device Discovery: The proposed solution must automatically accept log data from any system that is reporting through system. All log data, once received and indexed should be available for searches, alerts, and reports.		
160	System Process Status: The proposed solution must provide administration page that allows viewing underlying system process status and resetting application components. This should be provided through the same web interface along with all other administrative tasks.		

161	SSL Administration: Solution should have Self-signed certificate generation features so that accessing of appliance from client for monitoring and administration purposes can be done in encrypted manner.		
162	Administration Audit Trail: The proposed solution must log all administrative access and activities and provide access to the audit logs through the same web interface.		
163	Administration Alerting: The proposed solution must provide the ability to alert on system state activity such as low disk space, component failures, high resource utilization, etc. The transport for these alerts must be simple to configure and support SMTP, SNMP, Syslog, and/or direct SIEM		
164	The solution should provide intuitive mechanisms for troubleshooting such as proactive notifications, command line utilities etc		
165	The solution should support the automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, Bidder rule updates, device support, etc.		
166	Threat Hunting Features:		
a	The solution should have in-built ML based searches to perform threat hunting on 24x7 basis/real time		
b	The solution should give ability to perform open searches with simple and complex queries and enable threat hunting		
c	The solution should give ability to store queries and execute queries on a periodic basis/as per Data Centre requirement.		
d	The solution must give capability to perform manual and automated threat hunting		
e	The solution must have at least 500+ out of the box algorithms for Threat hunting which will execute queries on 24x7 basis		

SOAR Specification:

Sr . No	Specifications	Compliance Yes/No	Remarks
	General Requirement		
1	The solution must be a fully on-premise solution deployed in house. The OEM to provide the hardware for the proposed solution		
2	SOAR should be able to integrate bi-directionally with SIEM solution being proposed from day 1.		
3	The solution must be able to support creation of incidents via API, Web URL, SIEM, Ticketing system, manually etc.		
4	The solution must have capability to design workflow to provide fully automated action for the detected incident.		
5	The solution must have the capability to notify user based on detected/ identified incidents.		
6	Solution shall have the capability of providing independent threat intelligence for local and external threats.		
7	Solution should support deployment for access remote networks which are behind the firewall or isolated from Internet		
8	Solution should be able to integrate with security devices like Firewall, IDS/IPS, endpoint Security solution, APT solution, WAF, PIM etc from day one and the other proposed NG-SOC tools.		
12	The solution should provide for Threat Intelligence and Threat hunting capability via integration with the proposed TIP and Threat hunting platform.		
13	The solution must be web based without the need for installing an additional client software for administration and routine day to day usage requirements		
17	Solution should support backup / restore and provision for creating a HOT backup/standby server.		
18	Solution should support SAML 2.0 and Multi Factor Authentication		
19	The system should support a graphic UI for creations of playbooks		
20	The solution should support both human and machine-based automation for various tasks related to security investigations		
	Integration		

21	Solution should support integration with min 100 third party OEM products including but not limited to the following technologies. > Forensic tools > IT tools (AD, ISE, NOC tools) > Specify all products IT e.g. (AD, SAML) Communication tools (e.g.. Emails, SMS) SIEM tools. > Endpoint Security Solution > Network Security Solution > Threat Intelligence. > Dynamic malware analysis		
22	Solution should support adding of new product integrations and custom integrations.		
24	The solution should integrate with partner products using any of the standard protocols and interfaces including REST API, SOAP, SSH/CLI interface, and custom APIs.		
25	The solution must provide the capability to integrate multiple threat intelligence feeds from various providers to enrich incident artefacts.		
	Automation and Response		
26	The solution should provide a simple, comprehensive, fully automated approach to detect and stop the threats that matter, for on premise deployments from internal & external attacks on owner IT and OT system		
27	The solution should support both human and machine-based automation for various tasks related to security investigations		
28	Solution should support addition of automation scripts to existing integration		
29	For secure operations, the solution must run various scripts, commands, application functions, playbooks etc without the need of running with elevated privileges on a host OS		
30	Solution should use playbooks/runbooks with a visual editor/canvas which supports visual creation of playbooks without the need to code by native integration to third party tools and processes		
31	Solution should auto remediate the problem without causing a huge impact to the organization. Some of the examples such remediation could be: • Push policies to prevent an external IP • Isolate an internal desktop/Server • Disabling user accounts used for malicious purposes • Patch automation in case tool finds vulnerability		

BSES RAJDHANI POWER LIMITED

32	Solution should be configured with the used cases with automation for response to the minimum basic threats like: • Blacklisted IP Communication • Possible Penetration Testing Activity • Connection to Known Malicious Actor in Published Host List • DDOS Attack • Vulnerability scan detection • Phishing detection • Brute force attack • Malware /threat activity monitoring • Ransomware • Buffer Overflow attacks • Port & vulnerability Scans • Password cracking • Worm/virus outbreak • File access failures • Unauthorized server/service restarts • Unauthorized changes to firewall rules		
33	Solution should have min 30 built in reusable playbooks for well- known Incident types (Phishing, Malware, IOC Hunt) as per industry best practices		
34	Solution should allow creating new playbooks to map out the CIRT processes. Provision for building min 20 custom playbooks should be factored within the solution.		
35	Solution should support re-use of playbooks in bigger playbooks		
36	Solution Should allow creation of Manual Tasks, Automated Tasks and Conditional Tasks in Playbooks		
37	Automated and Manual Tasks within the same playbook		
38	Solution should allow a complete playbook to be run automatically or manually and list out any exceptions		
39	Solution must support step by step debugging of the running playbooks with provision of starting from where it stopped on error		
40	Solution should record all manual and automated entries during execution of a playbook		
41	Solution should allow addition of adhoc tasks within a playbook		
42	Solution must support provision to pass parameters to upstream/downstream task within a playbook.		
43	The solution must have an integrated versioning mechanism to save and maintain multiple versions for the playbooks.		

44	The solution should allow for viewing version history for all or selected playbook and provide option for restoring to an older version.		
45	Solution should be able to do incident analysis on the data received and should be an input for subsequent playbooks. The collected data can be used for incident analysis, and also as input for subsequent playbook tasks		
46	Solution should support updates for Playbooks, Integrations and should specify the procedure to update each of them.		
47	The solution should be able to find related incidents from historical data based on assets like IPs or user involved in incident		
48	The system should support parsing all the SIEM message fields, including but not limited to: creation time; update time; source/dest IP; source country; category; system; rule-name; severity; dest IP		
49	The system should support automatic reporting back to ticketing solution for example for closing cases state. These actions will be added to the audit trail.		
50	The solution should be able to consume security alerts/incidents from SIEM or directly from any other IT security solutions.		
51	Solution should support email or text notifications, along with functionality to email comprehensive periodic reports and dashboards.		
52	Solution should provide content for threat descriptions as well as remediation advice.		
53	Solution should provide necessary integration with the IT/ cyber security systems for keeping the forensics artifacts from the integrated sources of the incident before taking remedial actions.		
	Correlation & Analytics		
54	Solution should provide an integrated incident management platform for Security and IR team		
55	Solution should support assigning of incident to a User or a group		
56	Solution should maintain SLA for incident		
57	The solution must have a provision to remove duplicate incidents and merge all duplicate ones in a single incident automatically and manually.		
58	Solution should support highlighting of active incidents to quickly identify and access them.		

59	Solution should document all artifacts related to an incident		
60	Solution should support searching of Data/artifacts associated with historical incidents		
61	Solution should support visual mapping of an incident, its elements and correlated investigation entities, and the progression path of the incident, combining analyst intelligence with machine learning.		
62	Solution should support external users to contribute to an incident via email, message etc.		
63	Solution should highlight if any external products are required for Collaboration. It should provide an exhaustive list of such products currently supported.		
64	Solutions should support sharing of knowledge between users using its own platform		
65	Solution should provide an interface to drive High priority Security Incidents by Security teams and provide access and visibility of this incident to management, legal etc without any additional cost to licenses		
66	Solution should support key entities/IOCs for every incidents which can be auto extracted and presented in a graphical/ tabular form for analysts to view relationship between key entities for an incident.		
67	System should allow, more than 1 playbook to run on any incident. All execution logs should be retained and available for the reference.		
68	Solution should allow differentiation between alerts and incidents (incident could be made of multiple alerts.)		
69	The SOAR vendor should have In-built Automated Queue Management facility - Ability to create dedicated assignment queues and automated assignment and case progress with ease. Also helps in SOCs shift management		
70	The solution must provide periodic updates of playbooks, OEM supplied Integrations and threat intelligence for incident artefacts.		
71	The solution must support the ability to take-action related to an incident. For example, the solution should support the ability to block an intruder.		
72	The solution must support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution.		

73	The system should be able to extract IOCs from PDF/csv/other formats and search for those IOCs within the organization raw data. In case IOC is found, the system should trigger a new alert and save the indicator information in the local IOC Database.		
74	The system should support creation of an incident based on an email input (e.g. analyse all emails from a dedicated phishing mailbox)		
75	The system should have an option to edit and change the event properties (for example its severity).		
76	The solution must allow users to take remedial steps directly from within the visualization of incident correlation enabling a rapid and efficient response.		
77	Solution must provide for a dashboard for virtual War Room/ collaboration platform on a per incident basis for comprehensive collection of all investigation actions, artefacts, and collaboration at one place		
	Reporting		
78	The solution must provide reporting templates, to report on incident information, for the management team as well as the IT Security team via the GUI. Describe how the solution provides the ability to configure reports.		
79	The solution must provide configurable and customized report creation feature. Please describe how your solution meets this requirement.		
80	Solution should provide for documentation of evidence like IOCs, messages, running analysis on artifacts, notes, adding artifacts, etc) for later use for investigative purposes.		
81	Solution should record timestamp for all actions taken in an incident		
82	Solution should document all manual tasks perform by user in an incident		
83	Solution should provide Predefined reports		
84	Solution should support creation of customized reports in formats like csv, doc and pdf with custom logo of the organization		
85	Solution should support Dashboards which can provide high level view of Platforms KPI's to the management		
86	Solution should have documentation readily available for using automation and creation of custom automation		

87	Solution should provide integrated BI platform to help create advanced Dashboards and reports based on KPI's to be tracked		
88	Should support Custom Dashboards, Charts, Workflow and case management-Out-of-the-box Workflow templates for managing cases, Full featured case management platform that can integrate with external systems, Automated tasks within cases such as executing playbooks.		
	Administration and Configuration		
89	The solution must deliver customizable dashboard widgets that can present relevant incident information to the users.		
90	The solution must support a web-based GUI for management, analysis and reporting.		
91	The solution must provide central management of incidents and administrative functions from a single web-based user interface.		
92	Case Management: The proposed solution must provide complete process framework for integrating security monitoring and investigations with existing workflow procedures. Workflow should involve escalating an incident to other users within the same team or within other teams etc		
93	Workflow: The proposed solution should allow for assigning security analysts to specific security incident investigations. The proposed solution must provide a complete audit trail and accountability during the incident handling or forensic investigations. It should support the retrieval of relevant data to a cyber-security incident.		
94	Incident Tracking: The proposed solution must provide necessary tools to identify, isolate and remediate incidents as they occur.		
95	The solution should provide an web based tool for incident management and the same should follow industry best practices		
96	The administrator must be able to define role-based access to various functional areas of the solution. This includes being able to restrict a users access to specific functions of the solution that is not within the scope of a user's role including, but not limited to, administration, reporting, incident assignment, playbook creation.		
97	The solution must provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system.		
	Threat Intel Platform		

98	SOAR should have an integrated Threat Intelligence Platform (TIP) and should Facilitate importing and parsing structured and unstructured intelligence documents-Structured/finished intelligence analysis reports (.txt, .PDF); Automatically ingest email lists with threat information; Formatted CSV Files, XML-based structured intelligence –		
99	TIP should De-duplicate indicator input data when imported from multiple sources; Provide features to add context to and enrich threat intelligence-Ability to rank or assign severity of risk to intelligence and IOCs		
101	Support Integrations with Security Products-Native support for STIX/TAXII integrations, Export threat intel data with secure API, Integrate with additional tools and information sources via RESTful API		

UEBA (User Entity and Behavior Analytics) Specification:

Sr . No	Specifications	Compliance Yes/No	Remarks
1	On-premise deployment, with all the necessary components provided by the Bidder.		
2	Said UEBA tool should be able to integrate with Next Generation tools like NDR, SOAR & SIEM solution in		
3	The solution should be able to highlight risky and potentially abnormal user		
4	The solution should have permission for role based access including device admin, subnet admin, and should integrate audit logs, ability to edit model and advanced search, etc.		
5	Left Blank		
6	The agents of the solution should not be open sources, the agents should be from the same OEM and should not contain any malicious code. OEM to provide declaration for the same.		
7	Should be able to show us RAW and Normalized data, or relevant data basis on which anomalous behaviour was observed for a minimum of 180 days.		
8	Integration with enterprise authentication / SSO platform for simplified access		
9	Availability of out-of-the-box administrative dashboards and reports		
10	Identity based threat plane behaviour analysis for account hijacking and abuse		
11	Proactive and actionable alerting for anomalous behavior and risk scores		
12	High privilege access anomaly detection for misuse, sharing, or takeover		

13	Uses self-learning behavioral analysis to dynamically model each device, probabilistically identifying any anomalous activity that falls outside of the device's normal pattern of life.		
14	Unusual Credential use - models the times and devices normally used by each username, and alerts when there is an unusual combination		
15	Use of supervised machine / deep learning algorithms		
16	Flexibility to configure rolling window of period for behavior profiling		
17	Customizable dashboards, configurable policies and risk model optimization		
18	Ability to perform detailed search on raw and enriched data		
19	The solution should be an endpoint based UEBA, where the UEBA will take inputs from endpoint protection devices to further detect anomalies		
20	The solution should be installed passively into infrastructure		
21	The solution should be able to automatically identify and classify users and entities (i.e. devices, applications, servers, data, or anything with an IP address)		
22	Support highly available component architecture ensuring no single point of failure		
23	Exporting and report generation capabilities (Excel, PDF)		
24	The proposed solution must have built in File Integrity Monitoring, Process activity monitoring, Registry Integrity Monitoring with no additional cost		
25	Availability of out of the box reports for audit and compliance		
26	Ability to create custom reports and schedule the same		
27	Reports can be delivered as CSV, Email, PDF		
28	Ability to schedule reports with periodic intervals		
29	Usage changes over time: User activity deviates from normal over a short period of time or a gradual change over an extended period of time		
30	The solution must have the capability to perform a continuous evaluation of threat actor, and can cluster the behaviour and impacted entities, it can then build a baseline with ML capabilities and this baseline forms the input to detect sophisticated attacks. This process takes input from both internal and external threat intelligence sources.		
31	Change in account privileges: User attempts to change privileges on existing account or open new accounts on other systems		

32	Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing		
33	Sensitive data leakage: User manipulates http request / response parameter to download sensitive data		
34	UEBA should activate rules for a set of users until a specified condition or specified time window		
35	More data being transferred then a normal to and from servers and/ or external locations		
36	The proposed UEBA solution must include rule configuration management capabilities. It should allow users to create rules for entity mapping and profiling, provide the rule descriptions, mark the severity of alerts, select a risk category and tag configuration to generate ticket, schedule a mail etc.		
37	Should identify User involved in previously malicious or threatening behavior		
38	Detect insider threats, account hijacking and abuse, plus data exfiltration		
39	Work-centric UI with case management, or input to third-party solutions		
40	The solution should consist of a powerful visualization platform that enables threats being analyzed and investigated intuitively		
41	The solution should be able to administer from a web browser		
42	The solution’s UI should be able to provide a real-time, operational overview of an organization's entire network at any given time		
43	The solution’s UI should allow displaying threat by user, device with sorting and selected period		
44	The UEBA solution should have the capability to generate tickets based on custom rules defined by the organization		
45	The UEBA solution should have the multitenancy inbuilt to the platform.		
46	The UEBA should have the option to can configure rules based on individual tenants		
47	The solution’s UI should provide a Google-like search bar to search a device by Hostname, Mac Address, Username of user logged into that device, IP Address.		
48	Generate a threat Report which will look over a specified time period and produce a report based on the statistics generated.		
49	Allows us to create Incidents out of Events/alerts onto which analysts will collaborate inputs and for which, reports can be exported		
50	Multiple elements can be correlated into an incident alert		

BSES RAJDHANI POWER LIMITED

51	All the Event, Alerts and other information pertaining to Data Centre's NG-SOC must remain within Data Centre premises only. Any information moving out of Data Centre premises shall be reviewed and approved by the Data Centre on need basis.		
52	Use of supervised machine learning algorithms		
53	The solution must have the capability to perform a continuous evaluation of threat actor, and can cluster the behaviour and impacted entities, it can then build a baseline with ML capabilities and this baseline forms the input to detect sophisticated attacks. This process takes input from both internal and external threat intelligence sources. SOAR		

Network Detection and Response (NDR) Specifications:

Sr . No	Specifications	Compliance Yes/No	Remarks
1.1	Proposed NDR Systems should be hardware-based appliances.		
1.2	All systems / sub –systems of proposed NDR systems should have dual redundant hot swappable internal power supply.		
1.3	The proposed solution must support full packet capture and smart capture		
1.4	The solution should be sized for 2 Gbps from day one with ability to scale upto 10 Gbps in future.		
1.5	Bidder is to quote hardware appliances (i.e. Compute, Memory, storage, Operating Systems, DB, replication and corresponding licenses etc). Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. In case of any shortfall in hardware and software, the OEM will be responsible to supply additional hardware and software without any financial cost to User to ensure successful deployment of the NDR solution. All hardware and software components of appliance-based solutions must be hardened to ensure security of the system and all versions of OS/firmware/patch update schedule/ best practices must be shared by OEM with User.		
1.6	The system should be designed and deployed to work with the existing network and devices and should not require re-architecting the network or replacement of existing devices.		
1.7	Proposed NDR systems should not have any dependency on existing switching infrastructure including		

	but not limited to make, model, IOS, version etc.		
1.8	Responsibility of configuring the switches for successful deployment of proposed NDR systems lies with the bidder at BSES locations as applicable.		
2	**Visibility & Identity**		
2.1	The NDR tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NDR integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.		
2.2	The Network Detection and Response (NDR) solution should provide extensive flexibility and capability to delve deeply into end-user activities, MAC (Media Access Control) addresses, network flows, interface utilization, and a comprehensive range of other host statistics essential for swift incident resolution. It must leverage anomaly detection techniques to detect various types of attacks, including zero-day exploits, self-modifying malware, intrusions.		
2.3	The proposed solution must have the ability to natively monitor layer 7 traffic and perform deep packet inspection (DPI) without any 3rd party solution		
2.4	By collecting, analyzing and storing information from various sources, the NDR System should provide a full audit trail of all network transactions and perform more effective forensic investigations.		
3	**Functional Requirements**		
3.1	The solution should be able to provide real-time monitoring and visibility into all network traffic, using machine learning, context-aware analysis, and on-premise threat detection and analytics.		
3.2	Network Detection and Response (NDR) solutions leverage the inherent flow technologies present in network devices. These tools should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics, represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes.		
3.3	The solution should provide contextual network-wide visibility via an agentless approach.		
3.4	NDR solution should be able to use the existing network environment as a sensor grid to analyze traffic flow across the across the existing network and security solutions in a non-disruptive manner		
3.5	The solution should have an automated discovery function to identify network devices and capture		

	information such as IP address, OS, services provided, other connected hosts.		
3.6	The system should be able to monitor flow data between various VLANs.		
3.7	The solution should have the capability of application profiling in the system and also support custom applications present or acquired by the end user.		
3.8	The solution should have the capability to enrich flow records with additional fields including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, number of packets and number of bytes transmitted in a session, timestamps for start and end of session, NAT translations, etc. from captured data and then utilize those fields in analytical algorithms to alarm on anomalous behaviors.		
3.9	The solution must be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network.		
3.10	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL.		
3.11	The solution should be able to combine the flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation.		
3.12	The solution must be able to stitch flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.		
3.13	The solution must provide an application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.		
3.14	The solution must probe the network in a manner so that impact on network performance is minimal.		
3.15	The solution must be an out of band analytics engine from the primary data path.		
3.16	The system should provide detailed visibility to identify asset-based information within the network automatically.		
3.17	The solution should have capability to assign risk and credibility rating to alerts and present critical high-fidelity alerts prioritized based on threat severity with contextual information on the dashboard.		
3.18	The solution should provide use cases to identify usage of insecure, legacy and deprecated encryption algorithms being used by servers on the network.		
3.19	The solution should provide the capability to define custom policies to evaluate flow attributes such as bytes,		

BSES
RAJDHANI POWER LIMITED

	services, process, name and more.		
3.2	The solution must have the capability to identify network traffic from high risk applications such as file sharing, and perform a continuous evaluation of threat actors, and cluster the behaviour to detect sophisticated attacks.		
4	**Threat Detection Capabilities**		
4.1	The NDR solution should provide enterprise-wide network visibility and apply advanced security analytics to detect and respond to threats in real time. NDR solutions must be able to detect threats such as reconnaissance, data hoarding/exfiltration, distributed-denial-of- service (DDoS) attacks and insider threats.		
4.2	The solution should detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.		
4.3	Detect in-progress attacks as they evolve and a true 360° view in the networks like whom and what is really using your data or facilities.		
4.4	The solution must identify an attack on the corporate network using a RAT (Remote Access Tool) like unknown/known botnets.		
4.5	The solution must detect anomalous data transfer from/to the corporate network or within the network.		
4.6	The solution must detect unusual, unauthorized behavior within the network. This includes but is not restricted to unusual RDP, port scanning, unauthorized new devices plugged in, etc.		
4.7	Systems can produce detailed visibility to identify the endpoints and its information within the network automatically.		
4.8	System monitors traffic passively without being invasive on the network with the ability to send alerts in real time.		
4.9	System has the capability to historically track the location, dates first/last seen and summary of malicious activity.		
4.1	The solution should perform analysis on network data all the way up to the Layer 7 and provide complete application visibility		
4.11	The solution should be able to detect command and control bot communication based on the domain/url the user is trying to access.		
4.12	The solution should have DNS Threat Analytics Capability to detect the threat present in DNS traffic.		
4.13	The solution should have capability to detect DNS tunnelling.		
4.14	The solution should be able to detect vertical and horizontal scans within the environment		

BSES
RAJDHANI POWER LIMITED

4.15	The solution should highlight weak ciphers being used in the network by hosts or applications. The solution should search and monitor cipher suites and report on which ones are used on the network.		
4.16	The solution should be able to analyze SMTP traffic to detect high volume email, abnormal patterns in email traffic, traffic from unfriendly countries and with character sets often used by attackers (ex. Chinese).		
4.17	The solution should be capable of rejecting particular network data from analysis using input filters.		
4.18	It should have capability to detect and predict any data exfiltration by identifying abnormal behavior as part of cyber kill chain stages.		
4.19	The solution should support active scanning of specific enterprise assets in addition to passive profiling of devices on the network.		
4.2	Ability to detect ransomwares and profiling malwares such as Troldesh, Dridex, Quakbot, TrickBot, Gootkit, Adware, TorrentLocker, Adwind,Tofsee, Gozi, Jbifrost, Dyre, ZeuS Gameover, chinAd, bamital, Post Tovar GOZ, corebot, cryptominers, etc		
4.21	The solution must support VPN tunnel detection for private and anonymous VPN tunnels and just not the VPN used by the Organization. Privacy VPN - Personal VPN solutions which enable the user to avoid network monitoring solutions.		
4.22	The solution should support extraction of the payloads in the network traffic.		
4.23	The solution must support port-agnostic protocol detection. The solution should be capable of detecting protocols and applications despite them using non-standard TCP/UDP ports.		
4.24	NDR solution should provide a full-featured Network threat analyzer capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS).		
4.25	The NDR solution should be able to get threat intelligence from the research team to make detections of malware activity with higher accuracy and efficacy including Botnets, C&C servers, Bogons, Tor Entry/Exit Nodes, Connections to bad reputation Nations and Dark IPs..		
4.26	The solution must identify worms through techniques such as identifying the use of normally inactive ports or identification of network scanning activities.		
4.27	The solution should detect events of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including network flood events of ICMP, UDP, TCP SYN, TCP NULL, IP NULL, identify the presence of botnets in the network, etc. and detect long-lived connections that		

	may be associated with data-exfiltration.		
4.28	The solution must identify the presence of botnets in the network, DNS spoofing attack.		
4.29	The Solution must be capable of conducting protocol analysis to detect applications using unexpected ports, anomalous transfer of data via certain protocols indicative of tunnelling activity, backdoors, and the use of forbidden application protocols.		
4.3	The solution must utilize anomaly detection methods to identify attacks such as self-propagating malware and worms/viruses, lateral movement.		
4.31	The solution should support detection of malware in Encrypted traffic through analytics.		
4.32	The solution should be able to detect Unknown or encrypted malware, insider threats, policy violations.		
4.33	The Proposed solution should detect policy violations.		
4.34	Policy Violation detection rules should be modifyble to include Layer 7 details.		
4.35	The solution should provide a statistics based visualization for the better understanding of the policy based detection		
4.36	The system should able to provide the aggregated analysis for the policy violation and forensic		
5	**Integration**		
5.1	Solution shall support NTP server time synchronization.		
5.2	The NDR solution must be able to interoperate with the Data center, Core and Campus network to track endpoints and provide end-to-end visibility and control.		
5.3	The solution must integrate with existing security solutions like Security Information and Event Management (SIEM), Next-generation Firewalls, Router, Switches, NAC, SOAR, Proxy, WAF, mail gateway etc.		
5.4	The solution should have capability to instruct network security devices such as firewalls to block certain types of traffic, quarantine the host, etc.		
5.5	The solution should integrate with OpenLDAP, Microsoft Active Directory, RADIUS and DHCP to provide user Identity information in addition to IP address information throughout the system.		
5.6	The system should have a mechanism to consume external lists of known bad IP"s and generate alerts on the same if connection is seen.		
5.7	The NDR system should be able to integrate with external threat feeds.		
5.8	System should do event forwarding for SMTP, SYSLOG & SNMP for high risk issues.		
5.9	The solution should have native integration with CERT		

	CMTX & NCIIPC Threat Feeds		
6	**Reporting**		
6.1	Solution should have built-in various reports and can create custom reports like Executive report, detection life cycle report and Health reports etc.		
6.2	The solution should have the ability to generate reports in different formats, such as html, excel, csv and pdf. Reports should be available in real time on demand and should automatically be generated on a scheduled basis. Should support scheduled reports to be delivered via email automatically.		
6.3	Solution should come with predefined & customisable reports and should have ability to run certain reports based on security role.		
7	**Management**		
7.1	The proposed solution should have Centralized Management systems supporting role-based administration.		
7.2	The solution must be deployed in Centralized mode with central management and reporting from the single dashboard for the entire deployment.		
7.3	Enables administrators to centrally configure.		
7.4	The solution should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm.		
7.5	The solution should have an automated scanner to identify assets and should also be able to schedule the scans		
7.6	The solution should allow taking logs from proxy for the enrichment of the flows.		
7.8	The solution should offer country level traffic visibility and should have dedicated Country wise traffic dashboard		
7.9	The solution should have integration with the MITRE ATT&CK matrix		

BSES RAJDHANI POWER LIMITED

SECTION VI

PRICE BID

SECTION VI
PRICE FORMAT

S.No.	Description	Qty	Unit	Rate	Tax	Amount
	Part-A (Supply)					
1	Supply of SIEM & UEBA Solution with10000 EPS licenses	1	lot			
	(Provide price breakup separately in the block of 1000EPS)					
2	Supply of SOAR Solution (with 3 concurrent user license)	1	lot			
3	Supply of Network detection and response (NDR)	1	lot			
4	Hardware Appliance for SOC for S No. 1,2 & 3	1	lot			
	(Provide price breakup separately)					
5	Workstation for SOC monitoring:	3	Nos.			
	(Tower, Intel Xeon W3-2425, 16GB DDR4, 512GB M2 NVMe, NVIDIA Quadro NVS 450 2GB Graphics support dual HDMI monitor, Keyboard, Mouse, Win pro 11, 5 yrs warranty)					
6	27-inch FHD Monitor, IPS, 75 Hz, Bezel Less Design, AMD FreeSync, Flicker Free, HDMI, D-sub, 5 yrs warranty	6	Nos.			
7	85-inch industrial LED panel/screen for SOC with 2x2 screen splitter, 5 yrs warranty	1	No.			
	Total Part – A					
	Part-B (Installation, Commissioning and Testing)					
1	Installation, configuration and testing of SIEM, UEBA Solution	1	lot			
2	Installation, configuration and testing of SOAR Solution	1	lot			
3	Installation, configuration and testing of NDR Solution	1	lot			
	Total Part - B					

Part-C (SOC Operations)							
1	1^{st} year contract value for SOC Operations	1	Per annum				
2	2^{nd} year contract value for SOC Operations	1	Per annum				
3	3^{rd} year contract value for SOC Operations	1	Per annum				
	Total Part - C						
	Total Part A+B+C						
Part-D							
1	Additional 2-year Warranty and Support for SIEM, UEBA, SOAR, NDR complete solution along with hardware and software	1	lot				
2	Additional SOC Operations for 4^{th} and 5^{th} Year	2	Per annum				

NOTE:
1) The prices quoted are inclusive of training of BRPL officials (as per spec).
2) Qty Variation: The Company reserves the rights to vary the quantity by (+/-) 30% of the tender quantity.
3) The bidder shall, at its own, handle all imported equipment's and handle all formalities for custom clearances, port charges, etc. if any.
4) All Tools & Tackles, Consumables and Commissioning Spares required to complete the work shall be included in the quoted rates
5) Any other item not mentioned above but are required for successful completion of the works shall be deemed to be included in the above quoted rate
6) The payment for these items would be based on actual measurement wherever required.
7) The above quantities are indicative and may vary based on actual requirement while execution of work. The payment would be made as per actual.
8) Price Variation Clause: The prices shall remain firm during the entire contract period.
9) Penalty shall be levied on the basis of its performance mentioned in the Scope Section V and will be deducted accordingly from bill.

10) The bidder shall quote the prices strictly in the above format / item description / content. The bid shall be liable for rejection, if contractor fail to do so. If at any stage, the content is found to be changed from the given price format, the content as per the given price format will prevail and binding on the contractor.

11) The bidder needs to quote for all the line items as mentioned above; failing which the bids are liable for rejection.

12) RA is mandatory. The bids will be evaluated commercially based on the total value. RA methodology will be informed separately to all the qualified bidders. The original price bids of the bidders shall be reduced on pro-data basis against each line item based on the final all-inclusive prices offered during conclusion of the auction event for arriving at contract amount.

13) Commercial Bid will give the Total Price with item level breakup indicating the unit rate where applicable. It will include the following:

a. Hardware Cost
b. License Cost.

.

SECTION VII

VENDOR CODE OF CONDUCT

Purchaser is committed to conducting its business in an ethical, legal and socially responsible manner. To encourage compliance with all legal requirements and ethical business practices, Purchaser has established this Vendor Code of Conduct (the "Code") for Purchaser's Vendors. For the purposes of this document, "Vendor" means any company, corporation or other entity that sells, or seeks to sell goods or services, to Purchaser, including the Vendor's employees, agents and other representatives. Fundamental to adopting the Code is the understanding that a business, in all of its activities, must operate in full compliance with the laws, rules and regulations of the countries in which it operates. This Code encourages Vendors to go beyond legal compliance, drawing upon internationally recognized standards, in order to advance social and environmental responsibility.

I. Labour and Human Rights

Vendors must uphold the human rights of workers, and treat them with dignity and respect as understood by the international community.

- Fair Treatment - Vendors must be committed to a workplace free of harassment. Vendors shall not threaten workers with or subject them to harsh or inhumane treatment, including sexual harassment, sexual abuse, corporal punishment, mental coercion, physical coercion, verbal abuse or unreasonable restrictions on entering or exiting company provided facilities.
- Antidiscrimination - Vendors shall not discriminate against any worker based on race, colour, age, gender, sexual orientation, ethnicity, disability, religion, political affiliation, union membership, national origin, or marital status in hiring and employment practices such as applications for employment, promotions, rewards, access to training, job assignments, wages, benefits, discipline, and termination. Vendors shall not require a pregnancy test or discriminate against pregnant workers except where required by applicable laws or regulations or prudent for workplace safety. In addition, Vendors shall not require workers or potential workers to undergo medical tests that could be used in a discriminatory way except where required by applicable law or regulation or prudent for workplace safety.
- Freely Chosen Employment - Forced, bonded or indentured labour or involuntary prison labour is not to be used. All work will be voluntary, and workers should be free to leave upon reasonable notice. Workers shall not be required to hand over government-issued identification, passports or work permits as a condition of employment.
- Prevention of Under Age Labour - Child labour is strictly prohibited. Vendors shall not employ children. The minimum age for employment or work shall be 15 years of age, the minimum age for employment in that country, or the age for completing compulsory education in that country, whichever is higher. This Code does not prohibit participation in legitimate workplace apprenticeship programs that are consistent with Article 6 of ILO Minimum Age Convention No. 138 or light work consistent with Article 7 of ILO Minimum Age Convention No. 138.
- Juvenile Labour - Vendors may employ juveniles who are older than the applicable legal minimum age for employment but are younger than 18 years of age, provided they do not perform work likely to jeopardize

their heath, safety, or morals, consistent with ILO Minimum Age Convention No. 138.

- Minimum Wages - Compensation paid to workers shall comply with all applicable wage laws, including those relating to minimum wages, overtime hours and legally mandated benefits. Any disciplinary wage deductions are to conform to local law. The basis on which workers are being paid is to be clearly conveyed to them in a timely manner.
- Working Hours - Studies of good manufacturing practices clearly link worker strain to reduced productivity, increased turnover and increased injury and illness. Work weeks are not to exceed the maximum set by local law. Further, a work week should not be more than 60 hours per week, including overtime, except in emergency or unusual situations. Workers should be allowed at least one day off per seven-day week.
- Freedom of Association - Open communication and direct engagement between workers and management are the most effective ways to resolve workplace and compensation issues. Vendors are to respect the rights of workers to associate freely and to communicate openly with management regarding working conditions without fear of reprisal, intimidation or harassment. Workers' rights to join labour unions, seek representation and or join worker's councils in accordance with local laws should be acknowledged.

II. Health and Safety Vendors must recognize that in addition to minimizing the incidence of work-related injury and illness, a safe and healthy work environment enhances the quality of products and services, consistency of production and worker retention and morale. Vendors must also recognize that ongoing worker input and education is essential to identifying and solving health and safety issues in the workplace.

The health and safety standards are:

- Occupational Injury and Illness - Procedures and systems are to be in place to prevent, manage, track and report occupational injury and illness, including provisions to: a) encourage worker reporting; b) classify and record injury and illness cases; c) provide necessary medical treatment; d) investigate cases and implement corrective actions to eliminate their causes; and e) facilitate return of workers to work.
- Emergency Preparedness - Emergency situations and events are to be identified and assessed, and• their impact minimized by implementing emergency plans and response procedures, including: emergency reporting, employee notification and evacuation procedures, worker training and drills, appropriate fire detection and suppression equipment, adequate exit facilities and recovery plans.
- Occupational Safety - Worker exposure to potential safety hazards (e.g., electrical and other energy sources, fire, vehicles, and fall hazards) are to be controlled through proper design, engineering and administrative controls, preventative maintenance and safe work procedures (including lockout/tagout), and ongoing safety training. Where hazards cannot be adequately controlled by these means, workers are to be provided with appropriate, well-maintained, personal

protective equipment. Workers shall not be disciplined for raising safety concerns.

- Machine Safeguarding - Production and other machinery is to be evaluated for safety hazards. Physical guards, interlocks and barriers are to be provided and properly maintained where machinery presents an injury hazard to workers.
- Industrial Hygiene - Worker exposure to chemical, biological and physical agents is to be identified, evaluated, and controlled. Engineering or administrative controls must be used to control overexposures. When hazards cannot be adequately controlled by such means, worker health is to be protected by appropriate personal protective equipment programs.
- Sanitation, Food, and Housing - Workers are to be provided with ready access to clean toilet facilities, potable water and sanitary food preparation, storage, and eating facilities. Worker dormitories provided by the Participant or a labour agent are to be maintained clean and safe, and provided with appropriate emergency egress, hot water for bathing and showering, and adequate heat and ventilation and reasonable personal space along with reasonable entry and exit privileges.
- Physically Demanding Work - Worker exposure to the hazards of physically demanding tasks,• including manual material handling and heavy or repetitive lifting, prolonged standing and highly repetitive or forceful assembly tasks is to be identified, evaluated and controlled.

III. Environmental

Vendors should recognize that environmental responsibility is integral to producing world class products. In manufacturing operations, adverse effects on the environment and natural resources are to be minimized while safeguarding the health and safety of the public.

The environmental standards are:

- Product Content Restrictions - Vendors are to adhere to applicable laws and regulations regarding prohibition or restriction of specific substances including labeling laws and regulations for recycling and disposal. In addition, Vendors are to adhere to all environmental requirements specified by Purchaser.
- Chemical and Hazardous Materials -Chemical and other materials posing a hazard if released to the environment are to be identified and managed to ensure their safe handling, movement, storage, recycling or reuse and disposal.
- Air Emissions - Air emissions of volatile organic chemicals, aerosols, corrosives, particulates, ozone depleting chemicals and combustion by-products generated from operations are to be characterized, monitored, controlled and treated as required prior to discharge.
- Pollution Prevention and Resource Reduction -Waste of all types, including water and energy, are to be reduced or eliminated at the source or by practices such as modifying production, maintenance and facility processes, materials substitution, conservation, recycling and re-using materials.

- Wastewater and Solid Waste - Wastewater and solid waste generated from operations, industrial processes and sanitation facilities are to be monitored, controlled and treated as required prior to discharge or disposal.
- Environmental Permits and Reporting - All required environmental permits (e.g. discharge• monitoring) and registrations are to be obtained, maintained and kept current and their operational and reporting requirements are to be followed.

IV. Ethics

Vendors must be committed to the highest standards of ethical conduct when dealing with workers, Vendors, and customers.

- Corruption, Extortion, or Embezzlement - Corruption, extortion, and embezzlement, in any form, are strictly prohibited. Vendors shall not engage in corruption, extortion or embezzlement in any form and violations of this prohibition may result in immediate termination as an Vendor and in legal action.
- Disclosure of Information - Vendors must disclose information regarding its business activities, structure, financial situation, and performance in accordance with applicable laws and regulations and prevailing industry practices.
- No Improper Advantage - Vendors shall not offer or accept bribes or other means of obtaining undue or improper advantage.
- Fair Business, Advertising, and Competition - Vendors must uphold fair business standards in• advertising, sales, and competition.
- Business Integrity - The highest standards of integrity are to be expected in all business interactions. Participants shall prohibit any and all forms of corruption, extortion and embezzlement. Monitoring and enforcement procedures shall be implemented to ensure conformance.
- Community Engagement - Vendors are encouraged to engage the community to help foster social and economic development and to contribute to the sustainability of the communities in which they operate.
- Protection of Intellectual Property - Vendors must respect intellectual property rights; safeguard customer information; and transfer of technology and know-how must be done in a manner that protects intellectual property rights.

V. Management System

Vendors shall adopt or establish a management system whose scope is related to the content of this Code. The management system shall be designed to ensure (a) compliance with applicable laws, regulations and customer requirements related to the Vendors' operations and products; (b) conformance with this Code; and (c) identification and mitigation of operational risks related to this Code. It should also facilitate continual improvement.

The management system should contain the following elements:

- Company Commitment - Corporate social and environmental responsibility statements affirming Vendor's commitment to compliance and continual improvement.
- Management Accountability and Responsibility - Clearly identified company representative[s] responsible for ensuring implementation and periodic review of the status of the management systems.

- Legal and Customer Requirements - Identification, monitoring and understanding of applicable laws, regulations and customer requirements.
- Risk Assessment and Risk Management - Process to identify the environmental, health and safety and labour practice risks associated with Vendor's operations. Determination of the relative significance for each risk and implementation of appropriate procedural and physical controls to ensure regulatory compliance to control the identified risks.
- Performance Objectives with Implementation Plan and Measures - Areas to be included in a risk assessment for health and safety are warehouse and storage facilities, plant/facilities support equipment, laboratories and test areas, sanitation facilities (bathrooms), kitchen/cafeteria and worker housing /dormitories. Written standards, performance objectives, targets and implementation plans including a periodic assessment of Vendor's performance against those objectives.
- Training - Programs for training managers and workers to implement Vendor's policies, procedures and improvement objectives.
- Communication - Process for communicating clear and accurate information about Vendor's performance, practices and expectations to workers, Vendors and customers.
- Worker Feedback and Participation - Ongoing processes to assess employees' understanding of• and obtain feedback on practices and conditions covered by this Code and to foster continuous improvement.
- Audits and Assessments - Periodic self-evaluations to ensure conformity to legal and regulatory• requirements, the content of the Code and customer contractual requirements related to social and environmental responsibility.
- Corrective Action Process - Process for timely correction of deficiencies identified by internal or• external assessments, inspections, investigations and reviews.
- Documentation and Records - Creation of documents and records to ensure regulatory compliance• and conformity to company requirements along with appropriate confidentiality to protect privacy.

The Code is modelled on and contains language from the Recognized standards such as International Labour Organization Standards (ILO), Universal Declaration of Human Rights (UDHR), United Nations Convention against Corruption, and the Ethical Trading Initiative (ETI) were used as references in preparing this Code and may be useful sources of additional information.

BSES
RAJDHANI POWER LIMITED

Appendix- I

COMMERCIAL TERMS AND CONDITIONS – SUPPLY

Sl No	Item Description	AS PER BRPL	BIDDER'S CONFIRMATION
1	Validity	120 days from the due date of submission or amended due date of submission	
2	Price basis	a) **Firm**, FOR Delhi store basis. Prices shall be inclusive of GST, freight up to Delhi stores. b) Unloading at stores / site - in vendor's scope c) Transit insurance in BRPL scope	
3	Payment terms	As per Section-III, Clause: 8 (Terms of Payment and Billing).	
4	Delivery time	Within 45 days from date of PO/ LOI.	
5	Defect Liability period	As per Section-III, Clause: 13 (Warranty/Defects Liability Period)	
6	Penalty for delay	1% of basic price for every week delay subject to maximum of 10% of total PO/WO value of undelivered units/ remaining work.	
7	Performance Bank Guarantee	As per Section-III, Clause: 10 (Performance Gaurantee)	

Appendix- II

NO DEVIATION DECLARATION

NO DEVIATION –A (Technical)

NIT NO & DATE:

DUE DATE OF TENDER:

We hereby accept all terms and conditions of the technical scope of work as mandated in the tender documents subject to the following deviations as mentioned against the applicable technical qualifying requirement:

S.NO.	SL.NO OF TECHNICAL SPECIFICATION/SCOPE OF WORK	DEVIATIONS, IF ANY

SIGNATURE & SEAL OF BIDDER

NAME OF BIDDER

Note-The above template is indicative only, May vary depending on the nature of procurement/value.

NO DEVIATION –B (Commercial)

NIT NO & DATE:

DUE DATE OF TENDER:

We hereby accept all terms and conditions of the commercial requirement as mandated in tender document subject to the following deviations as mentioned against the applicable commercial qualifying requirement:

S.NO.	S. NO OF COMMERCIAL REQUIREMENTS	DEVIATIONS, IF ANY

SIGNATURE & SEAL OF BIDDER

NAME OF BIDDER

Note:-It is important to explicitly include all such terms and conditions which are considered absolutely necessary to be accepted by bidder without any deviation. Tender document shall have a stipulation that deviation to such criteria shall make the bid liable for rejection.

BSES
RAJDHANI POWER LIMITED

APPENDIX III

BID FORM

To,

Head of Department
Contracts & Material Deptt.
BSES Rajdhani Power Ltd
New Delhi 110019

Sir,

1 We understand that BRPL is desirous of execution of ………………………………………………………………………………(Name of work)

2 Having examined the Bidding Documents for the above named works, we the undersigned, offer to deliver the goods in full conformity with the Terms and Conditions and technical specifications for the sum indicated in Price Bid or such other sums as may be determined in accordance with the terms and conditions of the contract .The above amounts are in accordance with the Price Schedules attached herewith and are made part of this bid.

3 If our Bid is accepted, we under take to deliver the entire goods as) as per delivery schedule mentioned in Section IV from the date of award of purchase order/letter of intent.

4 If our Bid is accepted, we will furnish a performance bank guarantee for an amount of 10% (Ten) percent of the order value exclusive of GST for due performance of the Contract in accordance with the Terms and Conditions.

5 We agree to abide by this Bid for a period of 120 days from the due date of bid submission & subsequent corrigendum/amendment/extension of due date of submission. It shall remain binding upon us and may be accepted at any time before the expiration of that period.

6 We declare that we have studied the provision of Indian Laws for supply of equipments/materials and the prices have been quoted accordingly.
7 Unless and until Letter of Intent is issued, this Bid, together with your written acceptance there of, shall constitute a binding contract between us.
8 We understand that you are not bound to accept the lowest, or any bid you may receive.
9 There is provision for Resolution of Disputes under this Contract, in accordance with the Laws and Jurisdiction of Contract.

Dated this.............................. day of.. 20…..

Signature.. In the capacity of

……………………………..duly authorized to sign for

and on behalf of
(IN BLOCK CAPITALS)...

BSES
RAJDHANI POWER LIMITED

Appendix IV

ACCEPTANCE FORM FOR PARTICIPATION IN REVERSE AUCTION EVENT

(To be signed & stamped by the bidder along-with bid)

BSES Rajdhani Power Ltd (BRPL) intends to use reverse auction through SAP-SRM tool as an integral part of entire tendering process. All techno-commercially qualified bidders shall participate in the reverse auction.

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

1. In case of bidding through Internet medium, bidders are advised to ensure availability of all associated infrastructure as required to participate in the reverse auction event. Inability to bid due to telephone glitch, internet response issues, software & hardware hangs/failures, power failures or any other reason shall not be the responsibility of BRPL.
2. In case bidder fails to participate in the reverse auction event due to any reason whatsoever, it shall be presumed that the bidder has no further discounts to offer and the initial bid submitted by them as a part of tender shall be considered as bidder's Final No Regret offer. Any off-line price bids received from a bidder in lieu of non-participation in the reverse auction event shall be rejected by BRPL.
3. The bidder is advised to understand the auto bid process t safeguard themselves against any possibility of non-participation in the reverse auction event.
4. The bidder shall be prepared with competitive price quotes during the day of reverse auction event.
5. The prices quoted by bidder in reverse auction event shall be on FOR Landed cost BRPL Store/site basis inclusive of all relevant taxes, duties, levies, transportation charges etc.
6. The prices submitted by the bidder during reverse auction event shall be binding on the Bidder.

7. The bidder agrees to non-disclosure of trade information regarding bid details e.g. purchase, Identity, bid process/technology, bid documentation etc.

8. BRPL will make every effort to make the bid process transparent. However award decision of
BRPL will be final and binding on the bidder.

9. The prices submitted during reverse auction event shall be binding on the bidder.

10. No request for Time extension of the reverse auction event shall be considered by BRPL.

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

BSES
RAJDHANI POWER LIMITED

APPENDIX V

FORMAT FOR EMD BANK GUARANTEE

(To be issued in a Non Judicial Stamp Paper of Rs.50/-purchased in the name of the bank)

Whereas [*name of the Bidder*] (herein after called the "Bidder") has submitted its bid dated [*date of submission of bid*] for the supply of [*name and/or description of the goods*] (here after called the "Bid").

KNOW ALL PEOPLE by these presents that WE [name of bank] at [*Branch Name and address*],having our registered office at[*address of the registered office of the bank*](herein after called the "Bank"),are bound unto BSES Rajdhani Power Ltd., with it's Corporate Office at BSES Bhawan Nehru Place, New Delhi -110019 ,(herein after called —the "Purchaser")in the sum of Rs. ……………/- (Rupees ……………………………….. only) for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors, and assigns by these presents.

Sealed with the Common Seal of the said Bank this_____ day of________ 20____.

TH E CONDITIONS of this obligation are:

1 If the Bidder withdraws its Bid during the period of bid validity specified by the Bidder on the Bid Form ; or

2. If the Bidder, having been notified of the acceptance of its Bid by the Purchaser during the period of bid validity:

(a) Fails or refuses to execute the Contract Form, if required; or

(b) Fails or refuses to furnish the performance security, In accordance with the Instructions to Bidders/ Terms and Conditions;

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that is its demand the purchaser will note that amount claimed by it is due to it, owing to the occurrence of one or both of the two condition(s), specifying the occurred condition or condition(s).

This guarantee will remain in force up to and including One Hundred Twenty(120) days after the due date of submission bid, and any demand in respect thereof should reach the Bank not later than the above date.

(Stamp & signature of the bank)

Signature of the witness

BSES
RAJDHANI POWER LIMITED

APPENDIX - VI

LITIGATION HISTORY

Year	Name of client	Details of contract & date	Cause of Litigation/ arbitration and dispute	Disputed amount

APPENDIX - VII

CURRENT CONTRACT COMMITMENTS/ WORK IN PROGRESS

Year	Name of client	Details of contract & date	Value of outstanding work	Estimated completion date

APPENDIX - VIII

FINANCIAL DATA
(Duly Certified by Chartered Accountant)

	Actual in previous 5 financial years				
	FY 23-24	FY 22-23	FY 21-22	FY 20-21	FY 19-20
Total assets					
Current assets					
Total Liability					
Current Liability					
Profit before taxes					
Profit after taxes					
Sales Turnover					

APPENDIX-IX

FORMAT FOR PERFORMANCE BANK GUARANTEE

(TO BE ISSUED ON RS 1OO/- STAMP PAPER)

Bank Guarantee No.

Place:

Date:

To
BSES Rajdhani Power Limited

Whereas BSES RAJDHANI POWER LTD (hereinafter referred to as the "Purchaser", which expression shall unless repugnant to the context or meaning thereof include its successors, administrators and assigns) has awarded to M/s. with its Registered/Head Office at

(hereinafter referred to as the "Supplier" which expression shall unless repugnant to the context or meaning thereof, include its successors administrators, executors and assigns), a contract no. dated (the Contract);

And whereas the value of the Contract is Rs. (The Contract Value).

And whereas it is a condition of the Contract that the Supplier shall provide a Performance Bank Guarantee for the due and faithful performance of the entire purchase order for a sum equivalent to 10 % of the order Value exclusive of GST to the Purchaser.

And whereas the Bank under instructions from the Supplier has agreed to guarantee the due performance of the Contract.

Now it is agreed as follows:

1. We (Name of the Bank) having its Head Office at (hereinafter referred to as the Bank, which expression shall unless repugnant to the context or meaning thereof, include its successors, administrators, executors and assigns) 5hall indemnify and keep indemnified the Purchaser for, and guarantee and undertake to pay to the Purchaser immediately on written demand, a sum equivalent to % of the Contract Value
as aforesaid at any time upto (day/month/year) without any demur, reservation, contest, recourse or protest and/or without any reference to the Supplier, against all losses, damages, costs and expenses that may be caused to or suffered by the Purchaser by reason of any default on the pall of the Supplier in performing and observing any and allthe terms and conditions of the Contract or breach on the part if the Supplier of terms or conditions of the Contract.

2. The demand shall consist only of an original letter issued by Purchaser stating that the Supplier has failed to fulfill its obligations under the Contract. Such demand made by the Purchaser on the Bank shall be conclusive and binding notwithstanding any difference or dispute between the Purchaser and the Supplier or any difference or dispute pending before any Court, Tribunal, Arbitrator or any other authority.

3. The Bank undertakes not to revoke this guarantee during its currency without previous written consent of the Purchaser and further agrees that the guarantee herein contained shall continue to be enforceable during the period that would be taken for satisfactory performance and fulfillment in all respects of the Contract or in the event of any dispute between the Purchaser and Supplier until the dispute is settled (provided that d1e claim! demand under this guarantee is lodged /referred during the currency of this guarantee) or till the Purchaser discharges this guarantee whichever is earlier.

4. The Purchaser shall have the fullest liberty without affecting in any way the liability of the Bank under this guarantee from time to time to extend the time for performance of the Contract by tbe Supplier. The Purchaser shall have the fullest liberty, without affecting the liability of the Bank under this guarantee, to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the Supplier, and to exercise the same at any time in any manner, and either to enforce or to forbear to enforce any covenants, contained or implied, in the Contract. or any other course or remedy or security available to the Purchaser. The Bank shall not be released of its obligations under these presents by any exercise by the Purchaser of its liberty with reference: to the matters aforesaid or any of them or by reason of any other act or forbearance or other acts of omission or commission on the part of the Purchaser or any other indulgence shown by the Purchaser of by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the Bank.

5. The Bank agrees that the Purchaser and its option shall be entitled to enforce this guarantee against the Bank as a principal debtor, in the first instance without proceeding against the Supplier and notwithstanding any security or other guarantee that the Purchaser may hive in relation to the Supplier's liabilities.

6. Notwithstanding anything contained hereinabove the liability of the Bank under this guarantee is restricted to a sum equivalent to % of the Order Value ie. Rs.(Rupees) and it shall remain in force upto and including .Unless a demand to enforce a claim under this guarantee is made against the Bank within 3 months from the the above date of expiry i.e. up to all the rights of the Purchaser under the said guarantee shall be forfeited and the Bank shall be released and discharged from all liabilities thereafter.

7. This Performance Bank Guarantee shall be governed by the laws of India.

Dated this Witness

day of 20……. at

1. For Bank
2. Signature
Name Power of Attorney No:
Banker's Seal

BSES
RAJDHANI POWER LIMITED

APPENDIX-X

FORMAT FOR PRE BID QUERY SUBMISSION

S. No	Query Type Technical/ Commercial	Page No	Clause No	BRPL Clause	Bidder Query	Bidder Company Name	Bidder Contact Person	Bidder Contact No	Bidder Email ID
1.									
2.									
3.									

BSES
RAJDHANI POWER LIMITED

APPENDIX-XI

NON-DISCLOSURE AGREEMENT

(To be on a non-judicial stamp paper of Rs.100/-)

This agreement, made this ____ day of _________, 20___, at _________

BETWEEN

BSES Rajdhani Power Limited, a power utility Company incorporated under the provisions of the Companies Act, 1956 and having its registered office at BSES Bhawan, behind DTC Bus Terminal, Nehru Place, New Delhi-110019(hereinafter referred to as "BRPL"), which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors-in-business and assigns) and

AND

<Client Company Name>……………………………………..........................……………………………., a Company incorporated under the provisions of the Companies Act, <Year>............ and having its registered office at <Client Company Address> ......……………………..……………………...……………………………… ……….., (hereinafter referred to as "<Vendor"), which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors-in-business and assigns) of the Other Part;

WHEREAS:

"BRPL" a power utility Company is engaged in the business of Distribution of Electricity

A. "BRPL" requires the services of "<Client Company Name>………………………………………." for providing solutions which shall broadly focus on <purpose>…………………………………………………….. (hereinafter referred to as the "Purpose")

B. In the process of providing the services / proof of Concept for the purpose, BSES would provide and hand over to the "<Client Company Name>"………………………………………………………………… the personal, sensitive, confidential data, and Proprietary Information and Data relating to business operations of BSES, its customers and business associates and also technical and technological information and secrets belonging to BSES, its customers and business associates

C. BRPL desires to protect the said confidential and proprietary information and data as the disclosure of confidential information of BRPL to the industry, general public, or third parties could seriously jeopardize the intellectual property rights/ any other rights of BRPL.

NOW THIS AGREEMENT WITNESSETH AND IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES HERETO AS FOLLOWS:

1. The term "PERSONAL INFORMATION" and "SENSITIVE PERSONAL DATA" shall have the meaning as provided in The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 or as assigned in any other law in India and as amended from time to time.

2. The term "CONFIDENTIAL INFORMATION" shall include any confidential / proprietary / non-public information relating to the business of the respective parties, including but not limited to samples, formulae, manufacturing/development processes, specifications, drawings and schematics, however, the "Confidential Information" shall mean and include the technical and technological information and secrets relating to software, computer system, equipment, local area network and wide area network, network infrastructure and equipment, network designs/architecture, system passwords, login-ID's and commercial , marketing, financial and other information, data, ideas, programs, operations, processes and documents relating to the business or technology of (the "BRPL") or any of its affiliates which is disclosed either prior to or after the date of this Agreement by parties i) to each other ii) either of its affiliates or iii) a third party on or behalf of the BRPL or any of its affiliates, to the other party (the "Vendor") either in oral or written form, or through any other form of communication, and which was designated to be confidential and proprietary and shall include this Agreement as well as the intention of parties to explore the entering into of a business relationship with each other.

3. ACCEPTANCE TO BRPL INFORMATION SECURITY POLICY

   i. BRPL (BSES Rajdhani Power Limited) has legal ownership of the contents of all files created, processed, stored on its computers/ network systems as well as the data/ email/ messages transmitted in its network.
   ii. BRPL reserves the right to access the information given to the Vendor/ Consultant for processing without prior notice whenever there is a genuine need.
   iii. BRPL may in order to ensure cyber security/ protection of its data/ resources monitor, access, retrieve and read the information originating/ transmitted/ terminating in its network irrespective of user.
   iv. All the users accessing the network of BRPL are encouraged not to share their personal information on the computer/ network of BRPL computers, resouces and removable disks. If Users choose to share such personal information, the information may be monitored at the risk of Users.
   v. All users/vendors/consultants must return or ensure secure destruction of BRPL information, storage media, documentation, and computer/networking equipment in a permissible manner, before they leave a particular assignment, either on transfer or on the end of the contract or resignation.

vi. The undersigned has read the Information security policies and procedures and understand the policies and procedures of BRPL. The undersigned agreed to abide by the information security policies and procedures described therein as a condition of continued employment / contract. The Vendor undertakes to abide by all the rules and regulations applicable to Personal/ Sensitive/ Confidential Data under the Information Technology Act, 2000, or any other law as applicable from time to time and also the direction issued by the Regulator, Delhi Electricity Regulatory Commission.

vii. The BRPL has all the rights to claim damages for any loss of Personal/ Sensitive/ Confidential data including any liability arising to the third party due to the default/ failure of the Vendor to protect such data in terms of present agreement. The liability arising out of such default shall include the litigation cost, liability payable to third party and also any loss of reputation/ goodwill caused to the BRPL.

viii. That the Vandor agrees that the Non-compliance of the terms of this agreement and/or any of the policy of BRPL associated with the privacy policy, can result in disciplinary actions, revocation of systems privileges and includes termination of agreements/services, if any, claim of damages and such other actions as specified in other clauses of this agreement or the principle agreement.

4. EXCLUSIONS TO THE CONFIDENTIALITY AGREEMENT:

Notwithstanding anything contained herein, the obligation as to confidentiality herein shall not apply to the following, provided the VENDOR can establish the same with a competent proof, that:

a) the CONFIDENTIAL INFORMATION was already in the knowledge of the VENDOR, before its disclosure by the BRPL;
b) the CONFIDENTIAL INFORMATION, at the time of its disclosure by the BRPL to the VENDOR, was in public domain;
c) the CONFIDENTIAL INFORMATION became a part of public domain, after its disclosure by the BRPL to the VENDOR, either by publication or otherwise, except through the breach of this Agreement.
d) the CONFIDENTIAL INFORMATION was received by the VENDOR from a third party who was in possession of the same without violation of the obligation as to confidentiality;
e) the CONFIDENTIAL INFORMATION was independently developed by the VENDOR, without the breach of this Agreement;
f) the CONFIDENTIAL INFORMATION was required to be disclosed under the law;
The Information shall not be deemed to be in the public domain merely by the reason that it is known to a few members of the public to whom it might be of commercial interest. Further, a combination of two or more parts of the information

shall not be deemed to be in the public domain merely by the reason of each separate part thereof being so available in public domain.

5. OBLIGATIONS OF THE VENDOR

a. The VENDOR shall use the CONFIDENTIAL INFORMATION exclusively for its own purposes and shall not share the same otherwise to any third party, directly or indirectly, without the express consent of the BRPL (which consent may be withheld arbitrarily, and shall keep the same strictly confidential.
b. The VENDOR shall ensure that the CONFIDENTIAL INFORMATION is not accessible to any one other than those who are required to have such access for the purpose of the EVALUATION.
c. The VENDOR may disclose the CONFIDENTIAL INFORMATION to such of its employees or associates as are directly involved for the purpose of fulfilling the business association entered into between the parties on a need-to-know basis, provided that the VENDOR shall bind effectively such employees and / or such associates with a corresponding obligation. In any event, the VENDOR shall be responsible for any breach of this Agreement by any such employee or associate.
d. The VENDOR shall notify the BRPL upon its becoming aware of the occurrence of any breach of this Agreement due to any unauthorised use of CONFIDENTIAL INFORMATION.
e. The VENDOR shall not, without the written permission of the BRPL, make copies of the CONFIDENTIAL INFORMATION, or any part thereof.
f. In the event the VENDOR becomes legally compelled to disclose any CONFIDENTIAL INFORMATION, it shall promptly notify the BRPL about the same, so as to enable the BRPL to obtain appropriate protective order, if any. The VENDOR will exercise its best efforts to obtain assurance that confidential treatment will be accorded to the CONFIDENTIAL INFORMATION so disclosed, and shall make best efforts to diminish losses to the BRPL arising out of such disclosure. In any event, the VENDOR shall disclose only such part of the CONFIDENTIAL INFORMATION, as is legally mandatory.
g. The Vendor having access to Personal/ Sensitive/ Confidential data of BRPL shall apply security standards in a manner compatible to reasonable security standards as applied by the BRPL including ISO 27001 and other security policies and also in terms of Rule 8 of The Information Techonology (Resonable Sercurity Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The Vendors shall be responsible to ensure adherence to the security standards of all the access by their employees/ consultants etc
h. The Vendor shall securely delete the Personal/ Sensitive/ Confidential data which comes into its possession by virtue of this agreement and also sanitize the digital media as per the Security Policy of the BRPL.

6. The Vendor undertake to acquaint itself with the Information security policies and procedures and understand the policies and procedures therein which are published in

the intranet. The undersigned agreed to abide by the information security policies and procedures described therein as a condition of continued engagement/ contract.

7. RETURN OF CONFIDENTIAL INFORMATION

Immediately upon the decision by the VENDOR to not to continue with any any arrangement/ agreement or immediately upon the request of the BRPL, the VENDOR shall promptly return and/or procure the return of the CONFIDENTIAL INFORMATION, and all copies (whether or not lawfully made or obtained) of the same or any part of thereof, as well as all analysis, computations, studies or other documents or information prepared, which is based upon, contains or refers to or to any part of, the CONFIDENTIAL INFORMATION, to the BRPL or to any party designated by the BRPL in this behalf, or destroy the same as may be advised by the BRPL, and shall confirm by way of a written certificate to that effect to the BRPL, and also further confirm that the VENDOR has not reproduced or retained any samples, originals or copies of any part of the CONFIDENTIAL INFORMATION; except that the VENDOR could keep a single copy of the CONFIDENTIAL INFORMATION solely for the purposes of determining compliance with obligations as to confidentiality hereunder.

8. TENURE OF THE AGREEMENT

The Agreement shall be valid for a period of __________ years from the date thereof, or till parties enter into definitive Agreement of business relationship arising out of the or any earlier determination of this Agreement effected by the BRPL by requisitioning the return of the CONFIDENTIAL INFORMATION, whichever is earlier. The Vendor shall continue to be liable for any breach of Personal/ Sensitive/ Confidential data given by the BRPL even after the termination of main agreement.

9. WARRANTY AS TO ACCURACY OR COMPLETENESS OF THE INFORMATION

The BRPL makes no representation or warranty as to the accuracy or completeness of the CONFIDENTIAL INFORMATION disclosed to the VENDOR, and accordingly no liability accrues to the BRPL for any damage, injury or loss resulting from the use of the CONFIDENTIAL INFORMATION.

10. RELATIONSHIP PRESUMPTIONS

a. The VENDOR understands and acknowledges that nothing herein creates any presumptions about any proposed transaction or relationship with the BRPL.

b. This Agreement does not grant to the VENDOR any proprietary rights to the CONFIDENTIAL INFORMATION or any licence under any patents, trade marks, copyrights or any other intellectual property, and all right, title and interest in and to the CONFIDENTIAL INFORMATION shall remain the exclusive property of the BRPL.

c. Nothing in this Agreement shall be construed by implication or otherwise, as establishing any relationship of principal and agent or employer and employee between the parties hereto, or creating or authorising any party to create any commitment on behalf of the other party or any charge on the other party.

11. INJUNCTIVE RELIEF AND SPECIFIC PERFORMANCE

The VENDOR understands and acknowledges that, due to the unique nature of the CONFIDENTIAL INFORMATION of the BRPL, any unauthorised disclosure of any portion thereof shall cause irreparable damage / injury to the interest of the BRPL and that monetary relief will not be adequate or complete remedy to compensate for such damage/injury. Accordingly, the VENDOR hereby acknowledges that the BRPL shall be entitled to injunctive relief and / or a remedy of specific performance in the event of any unauthorised disclosure by the VENDOR or by any of its said employees or the said associates, in addition to whatever remedies it might have in law or in equity.

12. ENTIRE AGREEMENT

This Agreement represents the intentions of the parties hereto, in entirety, on the subject matter hereof, and shall supersede anything outside this Agreement relating to the subject matter hereof.

13. SEVERABILITY

If any part of this Agreement becomes or is discovered to be unlawful and / or unenforceable, and if the remaining Agreement could be separated from such part, then the remaining Agreement shall be deemed to continue in such reduced form.

Non-assignment - Save as expressly agreed by the parties hereto in writing, no right or obligation under this Agreement can be assigned to any other party.

Waiver - No waiver or modification of this Agreement will be binding upon the parties unless made in writing and signed by a duly authorised representative of such parties. Further, failure or delay in enforcing any right under this Agreement shall not amount to a waiver of such right.

Modifications - This Agreement may not be modified except in writing, signed by the parties hereto, through their duly authorised representatives.

Jurisdiction & Arbitration - This Agreement shall be governed by and construed in accordance with the Laws of India (without reference to the rules relating to the conflict of laws), under the jurisdiction of the Courts at Delhi.
Any dispute or difference with respect to the construction or interpretation of any of the clauses hereof, or as to the meaning or effect thereof, which could not be resolved amicably between the parties hereto, shall be referred to arbitration. The

arbitration shall be governed by the Arbitration and Conciliation Act, 1996, as amended or re-enacted. Each party hereto shall appoint one arbitrator. Both these arbitrators shall jointly appoint a third arbitrator. The Venue of arbitration shall be Delhi. The fees of the arbitrators shall be shared equally.

Related Party Acts -

a. Any act or omission which if it were an act or omission of the VENDOR would be a breach of this Agreement on its part, be deemed to be such an act or omission for which the VENDOR is responsible when done or omitted to be done by a third party, if –

i) such third party is controlled by or controls, the VENDOR, or

ii) both, such third party and the VENDOR, are under the common control of any other party

Two originals

This Agreement shall be executed in three copies, each of which shall constitute an original, and both of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by their duly authorised representatives, as on the date hereof.

For ______________________________ ______________________________ (name & title) Witnesses: 1. 2.	For <Client Company> ______________________________ ______________________________ (name & title) Witnesses: 1. 2.

****** End of BRPL NDA (Services) ******

BSES
RAJDHANI POWER LIMITED

APPENDIX-XII
BIDDER'S COMMUNICATION DETAILS

Bidder should furnish the below details for future communication: -

GENERAL INFORMATION	
NAME OF Company	
POSTAL ADDRESS	

FOR TECHNICAL QUERY:		
CONTACT PERSON & DESIGNATION	NAME	DESIGNATION
E-MAIL	MOBILE NO	TELEPHONE NO

FOR COMMERCIAL QUERY:		
CONTACT PERSON & DESIGNATION	NAME	DESIGNATION
E-MAIL	MOBILE NO	TELEPHONE NO

Note: No communication shall be entertained from any other email id, except as mentioned above. Bidder needs to inform the company if any changes in the email id on their letter head duly signed by the authorized signatory.

*****