BSES Yamuna Power Limited

NOTICE INVITING TENDER (NIT)

FOR

SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL

NIT NO: CMC/BY/24-25/RS/SkS/APT/48

[RFx Number: 2200000076]

Due Date for Submission: 02.01.2025, 15:00 HRS

BSES YAMUNA POWER LIMITED (BYPL)
CONTRACTS & MATERIALS DEPT.,
SHAKTI KIRAN BUILDING, KARKARDOOMA,
DELHI-110032
CIN: U40109DL2001PLC111525
WEBSITE: www.bsesdelhi.com

This document is a property of BYPL. This document is meant for the exclusive purpose of bidding against this NIT Number/Specification and shall not be transferred, reproduced, or otherwise used for purposes other than that for which it is specifically issued.

NIT INDEX

VOLUME – I: INFORMATION TO BIDDER (ITB)

SECTION – I: REQUEST FOR QUOTATION

1.00 EVENT INFORMATION

1.01 BSES Yamuna Power Ltd (hereinafter referred to as **"BYPL"**) invites **Open Tender** in the E-Tender Bidding Process on a "Single Stage: Two Parts" from interested Bidders to enter into the contract as detailed below:

Tender Description	Tender Fee (₹)	Estimated Cost (₹)	EMD Amount (₹)	Delivery at
Supply & Implementation of SoC Solution including technologies SIEM, SOAR, UEBA, NDR/NBAD, Threat hunting, Threat Intelligence, Incident Management for BYPL & BRPL	1,180	18.99 Crore	18.99 Lakh	Delhi Office(s)/ Site(s)

The bidder must qualify the requirements as specified in clause 2.0 stated below.

1.02 The tender document is available for downloading from our website www.bsesdelhi.com **--> BSES YAMUNA POWER LTD --> Tender --> Open Tenders** or through our E-Tendering portal link (https://srmprdportal.bsesdelhi.com).

1.03 **Tender Fee**: The bidder has to compulsorily submit the non-refundable tender fee of **₹ 1,180/-** as demand draft or online transfer of the requisite amount through IMPS/NEFT/RTGS covering the cost of bid documents. Any such bid submitted without this Fee shall be rejected.

1.04 **Earnest Money Deposit (EMD)** of ₹ 18,99,000/- (Rupees Eighteen Lakh and Ninety Nine Thousand only) valid for 120 days from the due date of bid submission in the form of BG/FD/online transfer of the requisite amount through IMPS/NEFT/RTGS. Any such bid submitted without EMD shall be rejected.

1.05 **TIME SCHEDULE**

The bidders should complete the following events within the dates specified as under:

S. No.	Events	Due date & Time
1	Date of availability of tender documents from BYPL Website & SRM	02.01.2025 up to 15:00 Hours
2	Date & Time of Pre-Bid Meeting Pre-Bid Meeting will be done online, Register in advance for this meeting via, the Zoom Meeting link: https://zoom.us/meeting/register/tJAucOipqTkoGt2CZqcB3dyW2OmTx90tZnsj After registering, you will receive a confirmation email containing information about joining the meeting.	24.12.2024, 15:00 Hours
3	Last Date of receipt of pre-bid queries, if any (Queries to be submitted via e-mail)	26.12.2024 up to 18:00 Hours
4	Last Date of replies to all the pre-bid queries as received	27.12.2024 up to 17:00 Hours
5	Last date and time of receipt of Complete Bids (Tender Fees, EMD, Part A & Part B)	02.01.2025 up to 15:00 Hours
6	Date & Time of Opening of PART A – EMD and Technical Bid	02.01.2025 up to 16:00 Hours
7	Date & Time of opening of Price/RA of qualified bids	Will be notified to the qualified bidders through our website/e-mail

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

The tender has been invited for both the discom i.e. BSES Yamuna Power Limited (BYPL) and BSES Rajdhan Power Limited (BRPL). All the tender process for both the discom will be carried simultaneously as per the process. After finalization of rates and agency for award, separate contracts will be awarded by both the discom.

All the clauses of this NIT, which are applicable to BYPL shall also be equally applicable to BRPL.

1.06 The Bid shall be submitted online in two (02) parts. Details of the parts are as follows:
Part A – Techno Commercial Bid
Part B – Price Bid
Bids will be submitted online and received up to **02.01.2025, 15:00 Hr.** at the address given below.
Part A of the Bid shall be opened online on **02.01.2025, 16:00 Hr.**
Part B of the Bid will be opened in case of Techno-Commercially Qualified Bidders and the date of opening of same shall be intimated in due course. It is the sole responsibility of the bidder to ensure that the bid documents are submitted online and reach this office on or before the last date.

Head of Department
Contracts & Materials Deptt.
BSES Yamuna Power Ltd
Reception, Ground Floor
Shaktikiran Building, Karkardooma
Delhi 110032

All envelopes shall be duly superscribed "**BID FOR SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL" "NIT NO: CMC/BY/24-25/RS/SkS/APT/48 [RFx Number: 2200000076] DUE ON 02.01.2025, 15:00 Hr.**"

1.07 BSES Yamuna Power Ltd reserves the right to accept/reject any or all tenders without assigning any reason thereof in the event of the following:

a) Tender is received after the due date and time.
b) Tender fee of requisite value is not submitted.
c) Earnest Money Deposit (EMD) of requisite value & validity is not submitted in the shape of a Bank Guarantee drawn in favour of BSES Yamuna Power Ltd, payable at Delhi or Online transfer of requisite amount through IMPS/NEFT/RTGS.
d) Price Bid as per the Price Schedule is not submitted.
e) Incomplete Bids.
f) Necessary documents against compliance to Qualification Requirements mentioned in Section 1 Clause 2.0 of this Tender Document.
g) Complete documents/details are not enclosed as per the Bid Index for Part-A (Technical Bid) at APPENDIX I ANNEXURE – 1.01.
h) Filled in Schedule of Deviations as per Annexure is not submitted.

2.00 QUALIFICATION CRITERIA

The prospective bidder must qualify for all of the following requirements and shall be eligible to participate in the bidding who meets the following requirements and management has a right to disqualify those bidders who do not meet these requirements.

2.01 Technical Criteria:

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 5 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 Authorised 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 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

2.02 **Commercial Criteria:**

S. No.	Criteria	Documents to be submitted by the bidder
8	The bidder should have average turnover of Rs. 50 Crores in at least three financial years last three years (i.e. 2021-22, 2022-23, 2023-24)	Balance Sheet / Copy of Audited P&L Account / Duly certified CA certificate having UDIN to be submitted
9	The Bidder should have a positive net worth in last three financial years (i.e. 2021-22, 2022-23, 2023-24)	Bidder should furnish a Certificate from the Chartered Accountant (CA) for Net Worth.
10	The bidder must have valid PAN No., GST registration in addition to other statuary compliance.	The bidder must submit the copy of registrations and submit an undertaking that the bidder shall comply all the statutory compliance as per the applicable laws/rules etc.
11	The Bidder shall submit an undertaking that "No Litigation" is pending with BYPL or its Group/ Associates Companies as on the date of bid submission	Self-undertaking on bidder's letterhead
12	The Bidder shall not be blacklisted/ debarred by any central/ state government institution /PSU/ electricity utilities as on the date of submission of the bid.	Self-undertaking on bidder's letterhead

Notwithstanding anything stated above, BYPL reserves the right to assess the bidder's capability to perform the contract, assess the capability and installed capacity of the Bidder for carrying out the supplies, should the circumstances warrant such assessment in the overall interest of the purchaser. In this regard the decision of the purchaser is final.

3.00 BIDDING AND AWARD PROCESS

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

3.01 BID SUBMISSION

BIDS ARE INVITED THROUGH THE E-PROCUREMENT PORTAL:
BSES will carry out E-Procurement through its e-procurement portal (https://srmprdportal.bsesdelhi.com).

Interested Non-registered bidders are requested to obtain the portal user name and password (if not available) for bid submission. For participating in e-Tenders of BYPL, please write a mail to
1. Mr Rakesh Sharma, E-mail: Rakesh.Ku.Sharma@relianceada.com,
2. Mr Anup Toppo, E-mail: Anup.toppo@@relianceada.com, with your details as per below:
a) Existing Vendor Code with BYPL or its Group/Associates Companies (if available): …………….
b) Trade Name: ………………………..
c) Address of Principal Place of Business: ………………………….

d) Contact Person's Name: ....
e) Contact Person's Designation: ....
f) Contact Person's Mobile No.: ....
g) Contact Person's email ID: ....
h) Also, attach a valid copy of the Power of Attorney in favour of the above-mentioned Contact Person for being authorized to receive user ID and password on behalf of their organization.

The login ID details shall be sent through email to the email ID mentioned by you for the same.

Bids shall be submitted in 2 (Two) parts on the assigned folder of the e-procurement site. Please refer to the user manual available at https://srmprdportal.bsesdelhi.com and enclosed with the tender.

Bids have to be mandatorily submitted only through the e-procurement portal of BSES Delhi. Bids submitted through any other form/ route shall not be admissible.

However, documents that necessarily have to be submitted in originals like Tender Fee (in the form of DD) or EMD (in the form of BG/FD/DD as applicable) and any other documents mentioned in the tender documents have to be submitted at the BYPL office before the due date & time of submission.

Please mention our NIT Number: - .... on the Tender and drop the same in our Tender Box placed at **BSES Yamuna Power Ltd, Reception, Ground Floor, Shaktikiran Building, Karkardooma, Delhi 110032**

The bids and the outer envelope shall be addressed to the following:
Head of Department
Contracts & Materials Deptt.
BSES Yamuna Power Ltd, Shaktikiran Building, Karkardooma, Delhi 110032
Kindly Note:

- The bidder has to ensure that the tender is dropped in the correct box designated for tender submission only.
- BYPL shall not be responsible for any wrong placement of tender documents by the bidder.

This is a two-part bid process. Bidders are to submit the bids online in 2(Two) parts **PART-A TECHNICAL BID & COMMERCIAL TERMS & CONDITIONS** and **Part-B FINANCIAL BID** and shall be submitted before the due date & time specified.

PART A: TECHNICAL BID comprising of the following, do not contain any cost information whatsoever and shall be submitted within the due date:

S. No.	Descriptions	Type of Documents/Format
A.1	Bid Details	
1	Bid Index for Part-A (Technical Bid)	In the prescribed format enclosed at APPENDIX I ANNEXURE – 1.01
2	Cover Letter, if any	Standard Format
3	Bid Form (Unpriced) Duly Signed	Duly Signed Bid Form as per enclosed format at APPENDIX I ANNEXURE – 1.02
4	Tender Fee	Non-refundable demand draft or online transfer of the requisite amount through IMPS/NEFT/RTGS for Rs 1,180/-, Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.03
5	EMD	Online transfer of the requisite amount through

		IMPS/NEFT/RTGS or FD or BG in the prescribed stamp paper & format enclosed at APPENDIX I ANNEXURE – 1.05, EMD Details Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.04
6	Power-of-Attorney/ Authorization Letter	In the standard stamp paper/letter
A.2	Technical Bid	
7	Communication Details of the Bidder	Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.06
8	Manufacturer Authorization Form (as applicable)	Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.07
9	Technical Qualifying Criteria Compliance Index & Documents	Documentary evidence in support of qualifying criteria mentioned in Section 1 Clause 2.00. Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.08, ANNEXURE – 1.09 & ANNEXURE – 1.10
10	Schedule of Deviations - Technical	Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.11
11	Technical Details/ Filled in Guaranteed Technical particulars (GTP) as per specification	Bidder shall submit duly filled GTP with all Technical documents (If Applicable)
12	Technical Drawings as per specification	Bidder shall submit all Drawings as per the specification (If Applicable)
13	Type Test Reports	Bidders shall submit a copy of type test reports in their technical bids in support of technical specifications. Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.12 (If Applicable)
14	Sample Submission Details (if applicable as per specification)	Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.13 (If Applicable)
15	Product Catalogue (If applicable)	Bidders shall submit a copy of the product catalogue in their technical bids in support of technical specifications
16	Manufacturer's Quality Assurance Plan	Bidders shall submit a copy of MQP in their technical bids in support of technical specifications
17	Other drawings/ documents mentioned in technical specification	Bidders shall submit a copy of documents in their technical bids in support of technical specifications(If Applicable)
18	Testing Facilities	Bidder shall submit the details of testing facilities available at their works/factory.
A.3	Commercial Bid	
19	Company Profile, Organization Chart & Manpower Details.	Bidder shall submit the details of Organization & Manpower with qualification and experience.
20	Commercial Qualifying Criteria Compliance Index & Documents	Documentary evidence in support of qualifying criteria mentioned in Section 1 Clause 2.00. Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.14
21	Undertakings	Duly signed self-undertakings as per enclosed format at APPENDIX I ANNEXURE – 1.15
22	Schedule of Deviations - Commercial	Duly filled and signed as per enclosed format at APPENDIX I ANNEXURE – 1.16

23	Acceptance Form For Participation in Reverse Auction Event	Duly signed Acceptance Form For Participation In Reverse Auction Event as per enclosed format at APPENDIX I ANNEXURE – 1.17
24	Commercial Terms and Conditions	Acceptance of Commercial Terms and Conditions viz. Delivery Schedule/Period, Payment terms, PBG etc. Duly filled and signed as per enclosed format at APPENDIX II ANNEXURE – 2.05
25	Un price Bid Duly Signed	Item wise marked as "Quoted" & Duly Signed Un price Bid as per enclosed format at VOLUME – II - PRICE BID FORMAT
26	Signed Tender document	Original Tender documents duly stamped & signed on each page as a token of acceptance

PART B: FINANCIAL BID comprising of

- Price strictly in the Format enclosed at VOLUME – II - PRICE BID FORMAT indicating Break up of basic price, taxes & duties, etc.
- The Bidder has to submit the item-wise price bifurcation in the bid. An unpriced copy must be attached with the Part A (Technical Bid).

This will be opened internally after techno-commercial evaluation and only of the qualified bidders.

REVERSE AUCTION CLAUSE: Purchaser reserves the right to use the reverse auction as an optional tool through SAP-SRM as an integral part of the entire tendering process. All techno-commercially qualified bidders shall participate in the reverse auction. Reverse Auction will be carried out on individual item-wise rates or Package-wise.

Notwithstanding anything stated above, the Purchaser reserves the right to assess the 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. Bidder is to submit their acceptance as per the format APPENDIX I ANNEXURE – 1.17.

BIDS RECEIVED AFTER THE DUE DATE AND TIME MAY BE LIABLE FOR REJECTION

4.00 AWARD DECISION

4.01 Purchaser intends to award the business on the lowest bid basis, so suppliers are encouraged to submit the bid competitively. The decision to place a Rate Contract/Purchase Order/LOI solely depends on the purchaser on the cost competitiveness across multiple lots, quality, delivery and bidder's capacity, in addition to other factors that Purchaser may deem relevant.

4.02 In the event of your bid being selected by the purchaser (and/or its affiliates) and you subsequent DEFAULT on your bid; you will be required to pay the 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.

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

4.04 Rate Contract: Not Applicable.

4.05 Rate shall remain FIRM till the validity of the Contract.

4.06 Quantity Variation: The purchaser reserves the right to vary the quantity by (±) 30% of the tender quantity during the execution of the rate contract.

4.07 Quantity Splitting: Not Applicable.

5.00 MARKET INTEGRITY

We have a fair and competitive marketplace. The rules for bidders are outlined in the Terms & Conditions. Bidders must agree to these rules before participating. 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. Bidders who violate the marketplace rules or engage in behaviour that disrupts the fair execution of the marketplace restrict a bidder to the length of time, depending upon the seriousness of the violation. Examples of violations include, but are not limited to:

- Failure to honour prices submitted to the marketplace.
- Breach of the terms of the published in Request for Quotation/NIT.

6.00 SUPPLIER CONFIDENTIALITY

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

All RFQ documents remain the property of BYPL and all suppliers are required to return these documents to BYPL upon request.

Suppliers who do not honour these confidentiality provisions will be excluded from participating in future bidding events.

7.00 CONTACT INFORMATION

Technical clarification, if any, as regards this RFQ shall be sought in writing and sent by e-mail/post/courier to the following addresses. The same shall not be communicated through phone

Address	Name/ Designation	E-mail Address
	Technical	
IT Dept. 3rd Floor, B-Block, BSES Yamuna Power Ltd Shaktikiran Building, Karkardooma, Delhi 110032	Lalit Kumar AsVP - Information & Technology	Lalit.V.Kumar@relianceada.com
	Ashwani Aggarwal Head - Information & Technology	Ashwani.aggarwal@relianceada.com
	Commercial	
C&M Dept. 3rd Floor, A-Block, BSES Yamuna Power Ltd Shaktikiran Building, Karkardooma, Delhi 110032	Anup Toppo Sr. Manager (C&M)	Anup.Toppo@relianceada.com
	Santosh Singh Addl. VP (Head-Procurement)	santosh.kum.singh@relianceada.com
	Robin Sebastian VP (HOD-C&M)	robin.sebastian@relianceada.com

SECTION – II: INSTRUCTION TO BIDDERS

A. GENERAL

1.00 BSES Yamuna Power Ltd, hereinafter referred to as "The Purchaser" is desirous of implementing the various Systems Improvement/Repair & Maintenance works at their respective licensed area in Delhi The Purchaser has now floated this tender for procurement of material notified earlier in this bid document.

2.00 SCOPE OF WORK

The scope shall include Supply & Implementation of SoC Solution including technologies SIEM, SOAR, UEBA, NDR/NBAD, Threat hunting, Threat Intelligence, Incident Management for BYPL & BRPL conforming to the Technical Specifications along with Packing, Forwarding, Transportation Unloading and proper stacking at Purchaser's stores/site.

3.0 DISCLAIMER

3.01 This Document includes statements, which reflect various assumptions, which may or may not be correct. Each Bidder/Bidding Consortium should conduct its 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 interest.

3.02 Neither Purchaser 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 Purchaser or its employees, or otherwise a rising in any way from the selection process for the Supply.

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

3.04 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).

4 COST OF BIDDING

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

B. BIDDING DOCUMENTS

5.01 The Scope of Work, Bidding Procedures and Contract Terms are described in the Bidding Documents.

5.02 The Bidder is expected to examine the Bidding Documents, including all Instructions, Forms, Terms and Specifications. Failure to furnish all information required by the Bidding Documents or submission of a Bid not substantially responsive to the Bidding Documents in every respect may result in the rejection of the Bid.

6.0 AMENDMENT OF BIDDING DOCUMENTS

6.01 At any time before the deadline for submission of Bids, the Purchaser may for any reason, whether at its initiative or in response to a clarification requested by a prospective Bidder, modify the Bidding Documents by Amendment.

6.02 The Amendment shall be part of the Bidding Documents, pursuant to Clause 5.01, and it will be notified on the website **www.bsesdelhi.com** and the same will be binding on them.

6.03 To afford prospective Bidders reasonable time in which to take the Amendment into account in preparing their Bids, the Purchaser may, at its discretion, extend the deadline for the submission of Bids. The same shall be published as a corrigendum on the website **www.bsesdelhi.com**

6.04 Purchaser shall reserve the rights to the following:
a) Extend the due date of submission,
b) Modify the tender document in part/whole,
c) Cancel the entire tender

6.05 **Bidders are requested to visit the website regularly for any modification/clarification/corrigendum/addendum of the bid documents.**

C. PREPARATION OF BIDS

7.0 LANGUAGE OF BID

The Bid prepared by the Bidder, and all correspondence and documents relating to the Bid exchanged by the Bidder and the Purchaser, shall be written in the English Language. Any printed literature furnished by the Bidder may be written in another language, provided that this literature is accompanied by an English translation, in which case, for purposes of interpretation of the Bid, the English translation shall govern.

8.0 DOCUMENTS COMPRISING THE BID

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

(a) All the Bids must be accompanied by the required Tender Fees and EMD as mentioned in the tender.
(b) PART A – Technical Bid and
(c) PART B - Financial Bid

9.0 BID FORM

9.01 The Bidder shall submit Bid Form with the Bidding Documents.

9.02 EMD

Pursuant to Clause 8.0(a) above, the bidder shall furnish, as part of its bid, an EMD amounting to as specified in Section I. The EMD is required to protect the Purchaser against the risk of Bidder's conduct which will warrant forfeiture.

The EMD shall be denominated in any of the following forms**:**

(a) Bank Guarantee drawn in favour of BSES Yamuna Power Ltd, payable at Delhi or
(b) Fixed Deposit (lien marked in favour of BSES Yamuna Power Limited) payable at Delhi.
(c) Online transfer of requisite amount through IMPS/NEFT/RTGS to BYPL account mentioned herein in Appendix II - **BYPL BANK DETAILS WITH IFSC CODE**.

EMD shall be valid for One Hundred Twenty (120) days after the due date of submission drawn in favour of BSES Yamuna Power Ltd.

The EMD may be forfeited in the case of:
(a) the Bidder withdraws its bid during the period of specified bid validity
or

(b) the case of a successful Bidder, if the Bidder does not

(i) Accept the Purchase Order, or

(ii) Furnish the required performance security BG.

10.0 BID PRICES

10.01 Bidders shall quote for the entire Scope of Supply/Work with a break-up of prices for individual items. 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, and Transportation to the site, all in accordance with the requirement of the Bidding Documents. The Bidder shall complete the appropriate Price Schedules included herein, stating the Unit Price for each item & total Price.

10.02 The prices offered shall be inclusive of all costs as well as Duties, Taxes or Levies paid or payable during the execution of the supply work, a 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.**

11.0 BID CURRENCIES

11.01 Prices shall be quoted in Indian Rupees Only.

12.0 PERIOD OF VALIDITY OF BIDS

12.01 Bids shall remain valid for 120 days from the due date of submission of the Bid.

12.02 Notwithstanding Clause 12.01 above, the Purchaser may solicit the Bidder's consent to an extension of the Period of Bid Validity. The request and the responses thereto shall be made in writing and sent by post/courier/E-mail.

13.0 ALTERNATIVE BIDS

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

14.0 FORMAT AND SIGNING OF BID

14.01 The original Bid Form and accompanying documents must be received by the Purchaser at the date, time and place specified pursuant to Clauses 15.0 and 16.0.

14.02 The original 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. The Bid submitted on behalf of companies registered with the Indian Companies Act, for the time being in force, shall be signed by persons duly authorized to submit the Bid on behalf of the Company and shall be accompanied by certified true copies of the resolutions, extracts of Articles of Association, special or general Power of Attorney etc. to show clearly the title, authority and designation of persons signing the Bid on behalf of the Company. Satisfactory evidence of the authority of the person signing on behalf of the Bidder shall be furnished with the bid. A bid by a person who affixes to his signature the words 'President', 'Managing Director', 'Secretary', 'Agent' or other designations without disclosing his principal will be rejected.

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

14.03 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 initiated by the person or persons signing the Bid.

D. SUBMISSION OF BIDS

15.0 SEALING AND MARKING OF BIDS

15.01 Bid submission: Bids have to be mandatorily submitted only through the e-procurement portal of BSES Delhi. Bids submitted through any other form/ route shall not be admissible.

15.02 However, documents that necessarily have to be submitted in originals like EMD or Tender Fee (in the form of BG/ DD /FD as applicable) and any other documents mentioned in the tender documents have to be submitted at the BYPL office before the due date & time of submission. The Technical Documents and the EMD shall be enclosed in a sealed envelope and the said envelope shall be superscribed with — "Technical Bid & EMD". All the envelopes should bear the Name and Address of the Bidder and mark for the Original. The envelopes should be superscribed with — "Tender No. & Due date of opening".

15.03 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 Purchaser to collect the proposals from Courier/Airlines/Cargo Agents etc. shall be entertained by the Purchaser.

16.0 DEADLINE FOR SUBMISSION OF BIDS

16.01 The Bid must be received by the Purchaser on or before the due date & time of submission.

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

17.0 ONE BID PER BIDDER

17.01 Each Bidder shall submit only one Bid by itself. No Joint venture is acceptable. A Bidder who submits or participates in more than one Bid will cause all those Bids to be rejected.

18.0 LATE BIDS

18.01 No Bid will be received by the Purchaser after the deadline for submission of Bids prescribed by the Purchaser, pursuant to Clause 16.0.

19.0 **MODIFICATIONS AND WITHDRAWAL OF BIDS**

19.01 The Bidder is not allowed to modify or withdraw its Bid after the Bid's due date & time of submission subject to any corrigendum/addendum/modifications in the tender documents uploaded to the website.

E. EVALUATION OF BID

20.0 **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 Purchaser's processing of Bids or award decisions may result in the rejection of the Bidder's Bid.

21.0 **CLARIFICATION OF BIDS**

To assist in the examination, evaluation and comparison of Bids, the Purchaser 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.

22.0 **PRELIMINARY EXAMINATION OF BIDS / RESPONSIVENESS**

22.01 Purchaser 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. Purchaser may ask for submission of original documents to verify the documents submitted in support of qualification criteria.

22.02 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.

22.03 Prior to the detailed evaluation, Purchaser will determine the substantial responsiveness of each Bid to the Bidding Documents including production capability and acceptable quality of the Goods offered. A substantially responsive Bid is one, which conforms to all the terms and conditions of the Bidding Documents without material deviation.

22.04 Bid determined as not substantially responsive will be rejected by the Purchaser and/or the Purchaser and may not subsequently be made responsive by the Bidder by correction of the non-conformity.

23.0 **EVALUATION AND COMPARISON OF BIDS**

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

23.02 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 will be subjected to a responsiveness check. The Technical & qualifying Proposals and the Conditional ties of the Bidders will 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.

23.03 The Purchaser'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 Bidding Documents

Bidders shall base their Bid price on the terms and conditions specified in the Bidding Documents.

The cost of all quantifiable deviations and omissions from the specification, terms and conditions specified in the Bidding Documents shall be evaluated. **The Purchaser will make its own assessment of the cost of any deviation to ensure a fair comparison of Bids.**

23.04 Any price adjustments that result from the above procedures shall be added for comparative evaluation only to arrive at an "Evaluated Bid Price". Bid Prices quoted by Bidders shall remain unaltered.

F. AWARD OF CONTRACT

24.0 CONTACTING THE PURCHASER

24.01 If any Bidder wishes to contact the Purchaser on any matter related to the Bid, from the time of Bid opening to the time of contract award, the same shall be done in writing only.

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

25.0 THE PURCHASER'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS

Submission of bids shall not automatically construe qualification for evaluation. The Purchaser reserves the right to accept or reject any Bid and to annul the Bidding process and reject all Bids at any time prior to the award of the 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 Purchaser's action.

26.0 AWARD OF CONTRACT

The Purchaser will award the Contract to the successful Bidder whose Bid has been Determined to be the lowest-evaluated responsive Bid, provided further that the Bidder has been determined to be qualified to satisfactorily perform the Contract. Purchaser reserves the right to award the order to other bidders in the tender, provided it is required for the timely execution of the project & provided he agrees to come to the lowest rate. Purchaser reserves the right to distribute the entire tender quantity at its own discretion without citing any reasons thereof.

27.0 THE PURCHASER'S RIGHT TO VARY QUANTITIES

The Purchaser reserves the right to vary the quantity i.e. increase or decrease the numbers/quantities without any change in terms and conditions during the execution of the Order.

28.0 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 responsive, techno-commercially acceptable and evaluated to be the lowest (L1). The successful Bidder shall be required to furnish a letter of acceptance within 7 days of the issue of the letter of intent /Notification of Award by Purchaser.

29.0 PERFORMANCE BANK GUARANTEE (PBG)

29.01 To be submitted within twenty-eight (28) days from the date of issuance of the Letter of Intent/Award/RC/PO. Bidder shall initially submit the performance bank guarantee (PBG) equivalent to 10% of total Purchase Order value (including GST) valid for a period of Sixty months (60) from the date of the commissioning or Sixty Six months (66) from the date of receipt of material (last consignment) at site/stores whichever is earlier plus 3 months towards claim period. Upon receipt of the PBG by BYPL, the EMD shall be released.

29.02 The Performance Bank Guarantee (PBG) shall be submitted separately against contracts for both discom.

30.0 CORRUPT OR FRAUDULENT PRACTICES

30.01 The Purchaser requires that the Bidders observe the highest standard of ethics during the procurement and execution of the Project. In pursuance of this policy, the Purchaser:

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

(i) "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 contract execution; and

(ii) "Fraudulent practice" means a misrepresentation of facts to influence a procurement process or the execution of a contract to the detriment of the Purchaser, and includes collusive practice among Bidders (before or after Bid submission) designed to establish Bid prices at artificial non -competitive levels and to deprive the Purchaser 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, 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.

30.02 Furthermore, Bidders shall be aware of the provision stated in the Terms and Conditions of the Contract.

31.0 STATUTORY GUIDELINES & REGULATIONS

The bidder shall make himself fully aware & familiarize himself with all applicable laws/ guidelines/ regulations.

32.0 SAFETY

Safety related requirements as mentioned in our safety Manual put on the Company's website which can be accessed at http://www.bsesdelhi.com. All bidders shall strictly abide by the guidelines provided in the safety manual at all relevant stages during the contract period.

33.0 PRIORITY OF CONTRACT DOCUMENTS

The several documents forming the Agreement are to be taken as mutually explanatory of one another, but in case of ambiguities or discrepancies, the same shall be explained and adjusted by the company, who shall, accordingly, issue suitable instructions thereon to the Contractor. In such event, unless otherwise provided in the agreement or explained by way of instructions by the company, as mentioned above, the priority of the documents forming the Agreement shall be as follows:

i) Contract Agreement/Purchase Order.
(a) Special Conditions of Contract
(b) General Conditions of Contract
(ii) The Letter of Acceptance/ Intent
(iii) Agreed Minutes of the Tender Negotiation Meetings
(iv) Agreed Minutes of the Tender Technical Meetings
(v) The Priced Bill of Quantities
(vi) The Technical Specifications / Scope of work
(vii) The Tender document, including all Appendices and/or Addenda, Corrigendum the latest taking precedence.

In the event of any conflict between the above-mentioned documents, the more stringent requirement or conditions which shall be favourable to the company shall govern and the decision of the company/BYPL shall be final and binding upon the parties.

APPENDIX I

ANNEXURE – 1.01

BID INDEX FOR PART-A (TECHNICAL BID)

(To be filled & submitted on Bidder Letter Head, Bidders document submission should have following main categories as outlined below and should have page numbers printed at the bottom of each page with this page as page number 1. The page number should be in "Page X of Y" format. Separator with document description shall be provided before each document)

NIT & RFX No.:

Bidder's Name:

Bidder's Bid Reference No. & Date:

S. No.	Particulars	Bid Pdf Page No.	
		From	To
A.1	**Bid Details**		
1.	Bid Index for Part-A (Technical Bid) as per APPENDIX I ANNEXURE - 1.01	1	
2.	Cover Letter, If any		
3.	Bid Form (Unpriced) Duly Signed as per APPENDIX I ANNEXURE - 1.02		
4.	Tender Fee Details as per APPENDIX I ANNEXURE - 1.03		
5.	EMD Details as per APPENDIX I ANNEXURE - 1.04 & 1.05		
6.	Power-of-Attorney / Authorization Letter		
A.2	**Technical Bid**		
7.	Communication Details of the Bidder as per APPENDIX I ANNEXURE - 1.06		
8.	Manufacturer Authorization Form (as applicable) as per APPENDIX I ANNEXURE - 1.07		
9.	Technical Qualifying Criteria Compliance Index & Documents as per APPENDIX I ANNEXURE - 1.08, 1.09, 1.10		
10.	Schedule of Technical Deviations (along with soft editable Excel copy) as per APPENDIX I ANNEXURE - 1.11		
11.	Guaranteed Technical particulars (GTP) as per specification (If Applicable)		
12.	All Drawings as per specification (If Applicable)		
13.	Type Test Reports (Sequence of Tests shall be strictly in accordance with relevant IS/IEC) as per APPENDIX I ANNEXURE - 1.12		
14.	Sample Submission Details (If applicable as per Specification) as per APPENDIX I ANNEXURE - 1.13		
15.	Product Catalogue (If applicable)		
16.	Manufacturer's quality assurance plan (as applicable)		
17.	Other drawings/ documents mentioned in technical specification		
18.	Testing Facilities		
A.3	**Commercial Bid**		
19.	Company Profile/Organogram/Organization Chart & Manpower Details		
20.	Commercial Qualifying Criteria Compliance Index & Documents as per APPENDIX I ANNEXURE - 1.14		
21.	Undertakings as per APPENDIX I ANNEXURE - 1.15		
22.	Schedule of Commercial Deviations (along with soft editable Excel copy) as per APPENDIX I ANNEXURE - 1.16		
21.	Acceptance form for participation in reverse auction event as per APPENDIX I ANNEXURE - 1.17		
24.	Acceptance of Commercial Terms and Conditions as per APPENDIX II ANNEXURE - 2.05		
25.	Un Price Bid Duly Signed (Volume - II Price Bid Format)		
26.	NIT Document complete Signed & Stamped		

ANNEXURE – 1.02

BID FORM

To

Head of Department
Contracts & Material Deptt.
BSES Yamuna Power Ltd
Shaktikiran Building, Karkardooma,
Delhi 110032

Sir,

1. We understand that BYPL is desirous of procuring……………………………………….………………….……. for it's licensed distribution network area in Delhi.
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 the Price Bid or such other sums as may be determined in accordance with the terms and conditions of the contract. The amounts are in accordance with the Price Schedules attached herewith and are made part of this bid.
3. If our Bid is accepted, we undertake to deliver the entire goods as per the delivery schedule mentioned in Section IV from the date of award of the purchase order/letter of intent.
4. If our Bid is accepted, we will furnish a performance bank guarantee for due performance of the Contract in accordance with the Terms and Conditions.
5. We agree to abide by this Bid for 120 days from the due date of bid submission and 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 the supply/services 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 thereof, 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, by the Laws and Jurisdiction of Contract.

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

Signature……………………………………….. In the capacity of ………………………………

…………………………………………………………duly authorized to sign for and on behalf of

(IN BLOCK CAPITALS)……………………………………………………………………..

ANNEXURE – 1.03

TENDER FEE DETAILS

a. Amount (Rs.) : **1,180/- (One Thousand One Hundred Eighty Only)**

b. Mode of Payment : DD or online transfer through IMPS/NEFT/RTGS (select any one)

c. DD /UTR No. (As applicable) : ……………………………………………………………………

d. Dated : ……………………………………………………………………

e. Bidders Bank Account No. : ……………………………………………………………………

f. Name of the Bank : ……………………………………………………………………

g. Address of the Bank : ……………………………………………………………………

h. IFSC Code of the Bank : ……………………………………………………………………

ANNEXURE – 1.04

EMD DETAILS

a. EMD Amount (Rs.) : ……………………………………………………………………

b. Mode of Payment : BG/FD/online transfer through IMPS/NEFT/RTGS (select any one)

c. BG/FD/UTR No. (As applicable): ……………………………………………………………………

d. Dated : ……………………………………………………………………

e. BG valid up to : ……………………………………………………………………

f. BG Claim period up to : ……………………………………………………………………

g. Bidders Bank Account No. : ……………………………………………………………………

h. Name of the Bank : ……………………………………………………………………

i. Address of the Bank : ……………………………………………………………………

j. IFSC Code of the Bank : ……………………………………………………………………

ANNEXURE – 1.05

(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*] (hereinafter called the "Bidder") has submitted its bid dated [*date of submission of bid*] for the supply of [*name and/or description of the goods*] (hereafter 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*] (hereinafter called the "Bank"), are bound unto BSES Yamuna Power Ltd., with its Corporate Office at Shaktikiran Building, Karkardooma, Delhi - 110032, (hereinafter 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____.

The 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 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

ANNEXURE – 1.06

COMMUNICATION DETAILS OF THE BIDDER

S. No.	Designation	Name	Mobile No.	E-mail id
1	CEO / MD			
2	Sales / Marketing Head			
3	Sales Representative / Key Account Manager (KAM)			
4	Technical Head			
5	Manufacturer Plant / Operations Head			
6	Post Order Execution In Charge			
7	Authorized contact person (Primary responsibility for the Bid)			
8	Authorized contact person (Secondary responsibility for the Bid)			

ANNEXURE – 1.07

MANUFACTURER AUTHORIZATION FORM
(To be submitted on OEM's Letter Head)

Date: …………….
Tender No.: …………..

To

Head of Department
Contracts & Material Deptt.
BSES Yamuna Power Ltd
Shaktikiran Building, Karkardooma,
Delhi 110032

Sir,

WHEREAS M/s. *[name of OEM]*, who are official manufacturers of ………… having factories at *[address of OEM]* do hereby authorize M/s *[name of bidder]* to submit a Bid in relation to the Invitation for Bids indicated above, the purpose of which is to provide the following Goods, manufactured by us ……………………………………………………………………………………………….and to subsequently negotiate and sign the Contract.

We hereby extend our full guarantee and warranty by the Conditions of the Contract or as mentioned elsewhere in the Tender Document, concerning the Goods offered by the above firm in reply to this Invitation for Bids.

We hereby confirm that in case, the channel partner fails to provide the necessary services as per the Tender Document referred above, M/s *[name of OEM]* shall provide standard warranty on the materials supplied against the contract. The warranty period and inclusion/exclusion of parts in the warranty shall remain the same as defined in the contract issued to our channel partner against this tender.

Yours Sincerely,

For ……………..

Authorized Signatory

ANNEXURE – 1.08

QUALIFYING CRITERIA COMPLIANCE INDEX - TECHNICAL CRITERIA				
S No	Qualifying Criteria Description as per section 1 clause 2.00	Documentary Proof Description	Documentary Proof Enclosed on Bid Page No.	
			From	To
1				
2				
3				
4				
5				

ANNEXURE – 1.09

LIST OF PURCHASE ORDERS EXECUTED & DELIVERY DETAILS IN SUPPORT OF QUALIFYING REQUIREMENTS													
S No	Item Details				PO & Execution Details					Customer Name	End User (shall be Utility/ SEB's/ PSU's) name and details	PO copy, MDCC /Delivery completion certificates/ Invoice Copies enclosed on Bid Page no.	
	Item	Model	Voltage Rating (kV)	Current Rating (A)	PO No	PO Date	PO Qty	Executed Qty	Execution Year			From	To
Total							∑	∑					

Note – Only items relevant as per qualifying requirements should be included in the list.

ANNEXURE – 1.10

LIST OF PERFORMANCE CERTIFICATES IN SUPPORT OF QUALIFYING REQUIREMENT														
S No	Item Details				PO No	Supplied/ Commissioning		Performance Certificate Issue Date	Performance Certificate Issued By End User (Utility/SEB/Govt Org.)	Contact Details of Issuing Person			Enclosed on Bid Page No.	
	Item	Model	Voltage Rating (kV)	Current Rating (A)		Qty.	Date			Name	Email	Mobile	From	To
Total						∑								

Note –

1. **Only items relevant as per qualifying requirement should be included in the list.**
2. **Only Performance certificates issued by End User (utilities/ SEB's/PSU's only) will be accepted as per qualifying requirement.**

ANNEXURE – 1.11

SCHEDULE OF DEVIATIONS - TECHNICAL

Vendor shall refrain from taking any deviations on this TENDER. Still, in case of any deviations, all such deviations from this tender shall be set out by the Bidder, Clause by Clause in this schedule and submit the same as a part of the Technical Bid.

Unless **specifically** mentioned in this schedule, the tender shall be deemed to confirm the BYPL's specifications:

Technical Deviations:-

S. No.	NIT Pdf Page No.	NIT Clause No.	NIT Clause Descriptions	Details of Clarification/deviation with justifications

Note – Please enclose detailed GTP and drawings as per specification after the technical deviation sheet

Seal of the Bidder:

Signature:

Name:

ANNEXURE – 1.12

TYPE TEST REPORTS (SEQUENCE OF TESTS SHALL BE STRICTLY IN ACCORDANCE WITH RELEVANT IS/IEC)								
S No	Test Description	Reference Standard	Reference Standard Clause No.	Name of Testing Lab	Test Report Reference Number	Date of Issue of Report	Report Enclosed on Bid Page No	
							From	To
1								
2								
3								
4								
5								
6								
7								

ANNEXURE – 1.13

SAMPLE SUBMISSION DETAILS (IF APPLICABLE AS PER SPECIFICATION)

S No	Description	Bidder's Response
1	Samples submitted with the bid	Yes/No
1	Sample Type -1	
1.1	Model Number	
1.2	Number of samples	
2	Sample Type -2	
2.1	Model Number	
2.2	Number of samples	

ANNEXURE – 1.14

QUALIFYING CRITERIA COMPLIANCE INDEX - COMMERCIAL CRITERIA

S No	Qualifying Criteria Description as per section 1 clause 2.00	Documentary Proof Description	Documentary Proof Enclosed on Bid Page No.	
			From	To
1				
2				
3				

ANNEXURE – 1.15

UNDERTAKINGS
(To be submitted on Bidders Letter Head)

Date: …………….

Tender No.: …………..

To

Head of Department
Contracts & Material Deptt.
BSES Yamuna Power Ltd
Shaktikiran Building, Karkardooma,
Delhi 110032

Sir,

We M/s *[name of bidder]*, ………… do hereby undertake that

- *[name of bidder]* has "No Litigation" pending with the BYPL or its Group/Associates Companies as on the date of bid opening.
- *[name of bidder] has* not been blacklisted/debarred by any central/state government institution/Electricity utilities as on the date of bid opening.
- *[name of bidder]* shall comply with all the statuary compliances as per the laws/rules etc. before the start of the supply/work.

Yours Sincerely,

For ……………..

Authorized Signatory

ANNEXURE – 1.16

SCHEDULE OF DEVIATIONS - COMMERCIAL

Vendor shall refrain from taking any deviations on this TENDER. Still, in case of any deviations, all such deviations from this tender shall be set out by the Bidder, Clause by Clause in this schedule and submit the same as a part of the Technical Bid.

Unless **specifically** mentioned in this schedule, the tender shall be deemed to confirm the BYPL's specifications:

Commercial Deviations:-

S. No.	NIT Pdf Page No.	NIT Clause No.	NIT Clause Descriptions	Details of Clarification/deviation with justifications

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

Seal of the Bidder:

Signature:

Name:

ANNEXURE – 1.17

ACCEPTANCE FORM FOR PARTICIPATION IN REVERSE AUCTION EVENT

(To be signed and stamped by the bidder)

BSES Yamuna Power Ltd (hereinafter referred to as **"BYPL"**) intends to use the reverse auction through the SAP-SRM tool as an integral part of the entire tendering process. All the bidders who are found as techno commercial qualified based on the tender requirements shall be eligible to participate in the reverse auction event.

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

1. BYPL shall provide the user ID and password to the authorized representative of the bidder. (Authorization letter in lieu of the same be submitted along with the signed and stamped acceptance form)
2. BYPL will make every effort to make the bid process transparent. However, the award decision by BYPL would be final and binding on the bidder.
3. The bidder agrees to non-disclosure of trade information regarding the purchase, identity of BYPL, bid process, bid technology, bid documentation, bid details, etc.
4. The bidder is advised to understand the auto bid process to safeguard themselves against any possibility of non-participation in the auction event.
5. In case of bidding through internet medium, bidders are further advised to ensure availability of the entire infrastructure as required at their end to participate in the auction event. Inability to bid due to telephone line glitches, internet response issues, software or hardware hangs; power failure or any other reason shall not be the responsibility of BYPL.
6. In case of intranet medium, BYPL shall provide the infrastructure to bidders, further, BYPL has sole discretion to extend or restart the auction event in case of any glitches in infrastructure observed which has restricted the bidders from submitting the bids to ensure fair & transparent competitive bidding. In case an auction event is restarted, the best bid already available in the system shall become the start price for the new auction.
7. In case the bidder fails to participate in the auction event due to any reason whatsoever, it shall be presumed that the bidder has no further discounts to offer and the initial bid as submitted by the bidder as a part of the tender shall be considered as the bidder's final no regret offer. Any offline price bids received from a bidder in lieu of non-participation in the auction event shall be outright rejected by BYPL.
8. The bidder shall be prepared with competitive price quotes on the day of the reverse auction event.
9. The prices as quoted by the bidder during the auction event shall be inclusive of all the applicable taxes, duties and levies and shall be FOR Landed Cost basis at the BYPL site.
10. The prices submitted by a bidder during the auction event shall be binding on the bidder.
11. No requests for time extension of the auction event shall be considered by BYPL.
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 the conclusion of the auction event to arrive at the contract amount.

Signature & seal of the Bidder

ANNEXURE – 1.18

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 Labor - 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 Labor - 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 health, 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 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 are 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) is to be controlled through proper design engineering and administrative controls, preventative maintenance and safe work procedures (including lockout/ragout), 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 are 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 by the Participant or a labour 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 a Vendor and in legal action.
- Disclosure of Information - Vendors must disclose information regarding their 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, and targets an 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 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

GENERAL CONDITIONS OF CONTRACT
(GCC- SUPPLY & IMPLEMENTATION)

GENERAL CONDITIONS OF CONTRACT (GCC)

The General Condition of Contract shall form a part of specifications, contract document.

1.0 General Instructions

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 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 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" shall mean BSES Yamuna 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 & Conditions, 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 BYPL in accordance with the specification.

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

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 the 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 supply, 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 in Section – IV of this RFQ.

4.03 Quantity variation and additional requirements if any shall be communicated to successful bidder during project execution.

4.04 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 of 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.

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 is to proceed with the work past a hold point only after clearance by purchaser or a witness waiver letter from BYPL.

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 that may be levied are to be borne by the bidder.

6.0 Inspection & Test Charges

6.01 GOODS shall be inspected by BUYER and/or third-party inspection agency nominated by BUYER. Inspection shall carry out stage-wise/final inspection as per agreed QA /QC procedure.
In addition, inspection of GOODS shall be carried out at our Site/stores. SELLER shall, however, repair/replace the damaged/rejected GOODS to the satisfaction of BUYER at no extra cost.

6.02 Inspection charges are included in total order value, however, BUYER will bear third-party inspection charges. In case of a futile/abortive visit of BUYER's inspector at SELLER'S works, the cost towards the same shall be debited from the SELLER's invoices.

6.03 GOODS covered by this PURCHASE ORDER shall not be dispatched in whole or in part until SELLER has received a written Release for Shipment Notice from BUYER or their designated representative.

6.04 Inspection call shall be raised a minimum of 7 (seven) days in advance from the delivery schedule mentioned in the PO and duly filled Format issued by BYPL

7.0 Handling and Storage

7.01 Material Safety Data Sheet (MSDS), detail handling & storage instruction sheet/manual, wherever applicable, to be furnished before the commencement of supply and one copy is to be submitted in store/site with First Lot.

8.0 Packing, Packing List & Marking

8.01 **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 BYPL, Delhi/New Delhi stores/site without undue risk of damage in transit. All the packaging materials as prescribed shall be supplied preferably with bio-degradable packing- materials.

8.02 **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.

9.0 Prices/Rates/Taxes

9.01 **Price basis for supply of materials**

a) Bidder to quote their prices on Landed Cost Basis and separate price for each item for supply to BYPL Delhi/New Delhi stores inclusive of packing, forwarding, loading at manufacturer's premises, payment of GST, Freight, and any other local charges. **Octroi is presently not applicable in Delhi and however if applicable shall be reimbursed at actuals.**

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

c) Transit insurance will be arranged by Bidder

10.00 Taxes & Duties

10.01 Prices for Goods are on Ex- Works basis. For the Goods covered under the GST laws, all taxes that are applicable under CGST, SGST, UGST, IGST and GST Compensation Cess shall be payable extra.

10.02 For the Goods not covered in the GST laws, the applicable ED, VAT / CST shall be payable extra at applicable rates.

10.03 GSTIN of BSES YAMUNA POWER LTD - 07AABCC8569N1Z0
CST No of BSES YAMUNA POWER LTD -07740254593
TIN NO of BSES YAMUNA POWER LTD - 07740254593
PAN NO of BSES YAMUNA POWER LTD - AABCC8569N

10.04 At the end of each month, the SELLER must submit their detail of invoices and amount thereof to the concerned officer in charge, within 07 days after the close of the respective month to which supply relates. Non-submission of the said request would be treated as good as the SELLER has no requirement for reconciliation.

11.0 Invoicing Instructions

11.01 Invoices in triplicate [1) Original for recipient, 2) Duplicate for Transporter, 3) Triplicate for supplier] shall be made out and delivered to the following address: BSES YAMUNA POWER LIMITED, SHAKTI KIRAN BUILDING, KARKARDOOMA, DELHI-110032.
MDCC will be released separately for Capex & Opex. Invoice will be submitted by the supplier as per the MDCC.

11.02 Vendor shall obtain GST registration in the State from where the supply will be carried out. Vendors supplying Goods to the Purchaser shall have a valid GST registration number and shall submit GST Tax Invoice and other documents as per SGST Act, CGST Act, IGST Act, UTGST Act, GST Compensation Cess Act and Rules made there under. Failure to submit GST Tax Invoice shall be liable for withholding SGST, CGST, IGST, UTGST, GST Compensation Cess amount charged by the vendor while releasing the payment.

11.03 Invoice will be in the name of BSES YAMUNA POWER LIMITED & address of the store/site mentioned in the MDCC. Invoice should contain all information as required under GST Invoice, Debit Note and Credit Rules. The government has notified rules of invoicing under GST along with a template of invoice(GST INV-01) covering the elements such as supplier's details, GSTIN No, HSN Codes, item details, GST tax rates, etc that need to be presented by the supplier.

11.04 Vendor to carefully examine and charge relevant CGST / SGST, UGST, IGST and GST compensation cess as applicable to the transactions.

11.05 Timely provision of invoices / Debit Notes / Credit Notes:

11.05.1 Vendor to timely provide invoice / Debit note / Credit note to enable Purchaser to claim tax benefit on or before stipulated time period. All necessary adjustment entries (Credit Notes, Purchase Returns, Debit Notes) shall be made within the timelines prescribed under the GST Laws.

11.05.2 In case of receipt of advance, the Vendor undertakes to raise the tax invoice. Purchaser, upon payment of advance, shall issue payment voucher as per applicable GST laws and rules. Four copies of the invoices need to be provided by suppliers and wherever the law requires, an Electronic Reference Number for each invoice.
Documents and devices to be carried by a person in charge of a conveyance under.

11.05.3 Any Vendors / Contractors / Service providers 'shall' mention the following minimum requirements in 'invoice' while furnishing Invoices with us:
1. Invoice / Credit Note Number and Date.
2. Address of supplier/service provider and GSTN.
3. Customer Name and Address as per GST Registration Certificate and GST registration Number.
4. 'Shipped to' and 'Billed to' addresses.
5. Place of Supply.
6. Description of Goods/Service along with unit of measurements.
7. HSN / SAC Code.
8. Taxable value (Gross & deduct Discount separately if allowed)
9. Rate and amount of Tax separately for CGST, SGST and IGST as applicable.
10. Signature of Supplier. (For e-invoices physical signature is not required)
11. Whether Reverse Charge is applicable or not.

11.06 E Way Bills/transit documents for movement of Goods:
Wherever applicable, the Vendor shall be responsible for issuing required transit documents / E Way Bills for the movement of Goods and the logistic partner/transporter shall not be liable for any loss arising due to confiscation of goods by government agencies on account of lack of proper documents or any misdeclaration. The Supplier is responsible for complying with rules applicable to the E-way bill. Any violation in provision of E-way Bill will attract penalties and seizure of Transit Material. Any Penalty and Pre-Deposit due to violation of rules/provisions shall be paid and borne by the Supplier. Also, the Supplier is responsible for releasing goods from the Authority whether CGST/SGST. Delay in supply from the contractual date due to the seizure of goods shall also attract liquidated damages.

12.0 Terms of Payment and Billing

12.01 Payment shall be made in milestone as per following:

➢ **<u>For Supply of Equipment's</u>:**

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 SIEM/SOAR hardware and licenses.
(iv) Submission of 10% PBG of part A for entire period of warranty 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 competition,
(iii) Approval of Administration & Operator's User's Manual,
(iv) Documentation & training.

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

➢ **<u>For Services (ITC)</u>:**

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

(i) Baseline system and application software installation, testing, commissioning, Review and Signoff.
(ii) Installation and Commissioning of SIEM/SOAR
(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 competition,
(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 months of successful system run

➢ **<u>For SOC Operations</u>:**

Bidder require to submit 10% of PBG of Contract value for full contract period.
Quarterly payment of yearly value will be paid in arrears (i.e end of quarter) on submission of all SLA reports.

Payment of SOC (Operation service) shall be after the go live after submission of PBG separately for Soc amount.

Note: Milestone payments shall be made in full upon the successful completion of the milestone. In the event that only a minor portion of a milestone is not fully completed, invoicing for partial payment of the milestone will be entirely to BYPL discretion. Payment terms shall be within 45 days from receipt of invoice supported by BYPL certification of completion of milestone.

Bidder to submit the following documents against dispatch of each consignment at our Vendor Support Cell (VSC):

a) Signed copy of accepted Rate 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 BYPL Store & Original certificate issued by BYPL 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.

12.02 Purchaser has the right to recover tax loss, interest and penalty suffered due to any non-compliance 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.

12.03 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.

12.04 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.

12.05 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".

13.0 Tax Indemnity Clause

13.01 Vendor (along with its affiliates in India or overseas including any agent/ third party contractor or any other person appointed by such affiliates for this agreement) agrees that it will be solely responsible for performing all compliances and making payments of all taxes (direct tax or indirect tax including but not limited to income-tax, transfer pricing, value added tax, SGST, CGST, IGST, UTGST, GST Compensation Cess custom duty, excise duty, Research and Development Cess, etc.), cesses, interest, penalties or any other tax/ duty/ amount/ charge/ liability arising either out of laws/ regulations applicable in India and overseas or because of a demand/ recovery initiated by any revenue authority under laws/ regulations applicable in India or overseas.

13.02 In case any tax liability (including but not limited to income tax, transfer pricing, value added tax, SGST, CGST, IGST, UTGST, GST Compensation Cess, custom duty, excise duty, Research and Development Cess, etc.), cesses, interest, penalties or any other tax/ duty/ amount/ charge/ liability becomes payable by Purchaser due to failure of the Vendor, or any of its affiliates in India or overseas including any agent/ third party contractor or any other person appointed by such affiliates for this agreement, to comply with the relevant laws/ regulations applicable in India or overseas, Vendor undertakes to indemnify Purchaser for an amount equal to amount payable by Purchaser.

13.03 Further, Vendor undertakes to keep Purchaser indemnified at all times against and from all other actions, proceedings, claims, loss, damage, costs and expenses which may be brought against Purchaser or suffered or incurred by Purchaser and which shall have arisen either directly or indirectly out of or in connection with failure of The Vendor, or any of its affiliates in India or overseas including any agent/ third party contractor or any other person appointed by such affiliates for this agreement, to comply with relevant obligations/ compliance under any law/ regulations applicable in India and overseas.

13.04 The parties agree to follow the following process in case any communication of demand, arising out of non-compliance by Vendor (along with its affiliates in India or overseas including any agent/ third party contractor or any other person appointed by such affiliates for this agreement), is received by Purchaser:

13.04.1 On Purchaser receiving any communication from a competent authority demanding tax liability (including but not limited to income tax, transfer pricing, value added tax, SGST, CGST, IGST, UTGST, GST Compensation Cess custom duty, excise duty, Research and Development Cess, etc.), cesses, interest, penalties or any other tax/ duty/ amount/ charge/ liability, Purchaser shall, within 5 common working days from the date of receipt of such communication (save where the period to respond to the relevant authority is less than five days, in which case, as soon as reasonably possible) inform Vendor in writing of such communication.

13.04.2 Pursuant to receiving communication from Purchaser, Vendor shall suggest to accept the communication and pay the demand amount to the competent authority. In such an event, Vendor shall reimburse such amount paid to Purchaser within 5 working days from the date of payment by Purchaser to the competent authority.

13.04.3 If Vendor advises in writing and Purchaser agrees to dispute the demand, then Purchaser shall dispute the matter with competent authority as per due process prescribed under the regulations and Purchaser shall not pay the Tax Demand. In such scenario, cost of litigation including but not limited to Counsel cost, filing fees, other related charges, should be reimbursed by Vendor to Purchaser. Additionally, If any coercive steps of recovery are initiated by the department, then Purchaser would pay such amount (including by way of adjustment of refunds due to it) and the same would be reimbursed by Vendor within 5 working days from date of such recovery from Purchaser. Purchaser will take all necessary steps to avoid such recovery measures.

13.04.4 On determination of the demand through an Order issued by a Tribunal or any other similar Authority, by whatever name called, under any law applicable in India or overseas, if the demand or any part thereof becomes payable and is paid by Purchaser, then Vendor undertakes to reimburse such amount to Purchaser within 10 days from the date of payment. Alternatively, if on determination of the demand through an Order, no amount is payable by Purchaser then any refund arising to Purchaser due to such an Order shall be passed on to Vendor within 10 days from the date of receipt of refund.

14.0 The Micro, Small and Medium Enterprises (MSME)

14.01 If the SELLERS establishment is covered under the purview of The Micro, Small and Medium Enterprises Development Act, 2006 and its amendments, he shall declare so within the bid of its status failing which it will be presumed that it is a non-MSME unit. Also, submit a copy of Udyog Aadhaar (UA) & Udyam Registration Number.

15.0 Price Validity

15.01 All bids submitted shall remain valid, firm and subject to unconditional acceptance by BYPL Delhi for 120 days from the due date of submission. For awarded suppliers, the prices shall remain valid till contract completion.

16.0 Performance Guarantee

16.01 To be submitted within twenty-eight (28) days from the date of issuance of the Letter of Intent/Award/RC. Bidder shall initially submit the performance bank guarantee (PBG) equivalent to 10% of total Purchase Order value (including GST) valid for a period of Sixty months (60) from the date of the commissioning or Sixty Six months (66) from the date of receipt of material (last consignment) at site/stores whichever is earlier plus 3 months towards claim period. Upon receipt of the PBG by BYPL against contract, the EMD shall be released.

16.02 Bank guarantee shall be drawn in favour of BSES Yamuna Power Ltd as applicable. The performance bank guarantee shall be in the format specified by BYPL.

16.03 The Performance Bank Guarantee shall be submitted against contracts separately for both discom

17.0 Forfeiture

17.01 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 BYPL 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 outlined in the Contract.

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

18.0 Release

18.01 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 16.0) except for the case outlined in Clause 22.0.

19.0 Defects Liability Period/Guarantee/Warranty & Support

19.01 Proposed solution should be with OEM warranty and support. Bidder required to provide OEM warranty certificate.

19.02 24x7, 4 hrs resolution, 5 years onsite Warranty (part and labor), support from OEM along with all patches for hardware and software

20.0 Return, Replacement or Substitution

20.01 BYPL shall give Supplier notice of any defective Commodity promptly after becoming aware thereof. BYPL may at its discretion elect to return defective Commodities to Supplier for replacement, free of charge to BYPL or may reject such Commodities and purchase the same or similar Commodities from any third party. In the latter case, BYPL 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. BYPL may set off such costs against any amounts payable by BYPL to the Supplier. Supplier shall reimburse BYPL for the amount, if any, by which the price of a substitute Commodity exceeds the price for such Commodity as quoted in the Bid. BUYER at its sole discretion shall have the opinion to dispose of the material or GOODS so rejected and not taken back within forty-five days from the date of intimation of rejection.

21.0 Effective date of commencement of contract

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

22.0 Time – The Essence of Contract

22.01 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.

23.0 The Laws and Jurisdiction of Contract:

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

23.02 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 Delhi, India

24.0 Events of Default

24.01 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 BYPL.

25.0 Consequences of Default.

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

(b) In the event of an Event of Default, BYPL 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 payment 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 BYPL may incur as a result of Supplier's default.

26.0 Penalty for Delay

26.01 If supply of items/equipments is delayed beyond the supply schedule as stipulated in the purchase order then the Supplier shall be liable to pay to the Purchaser as penalty for delay, a sum of 1% (one percent) of the basic (ex-works) price for every week delay of undelivered units or part thereof for individual milestone deliveries.

26.02 The total amount of penalty for delay under the contract will be subject to a maximum of ten percent (10%) of the basic (ex-works) price of total undelivered units.

26.03 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.

26.4 If the Penalty is levied as per the Order terms & conditions; BYPL will raise the Invoice for the penalty amount along with applicable GST rates. Accordingly, after setting off the penalty Invoice amount, net payment shall be made.

27.0 Variation in Taxes, Duties & Levies

27.1 The total order value shall be adjusted on account of any variations in Statutory Levies imposed by Competent Authorities by way of fresh notification(s) within the stipulated delivery period only. In case of reduction in taxes, duties and levies, the benefits of the same shall be passed on to BUYER.

27.2 No other Taxes, Duties or levies other than those specified above will be payable by BUYER except in case of new Levies, Taxes or duties imposed by the Competent Authorities by way of fresh notification(s) after the issue of PURCHASE ORDER but within the stipulated delivery period.

27.3 Notwithstanding what has been stated above, changes in Taxes, Duties & Levies shall apply only to that portion of PURCHASE ORDER not executed on the date of notification by the Competent Authority. Further, changes in Taxes, Duties & Levies after the due date of Delivery shall not affect PURCHASE ORDER Terms and Value.

27.4 PURCHASE ORDER value shall not be subject to any variation on account of variation in Exchange rate(s).

28.0 Taxes & Duties on raw materials & bought out components

28.01 Taxes & Duties on raw materials & bought-out components are included in Order Value and are not subject to any escalation or variation for any reason whatsoever.

28.02 Taxes & Duties on raw materials & bought-out components procured indigenously are included in Order Value and are not subject to any escalation or variation for any reason whatsoever.

29.0 Force Majeure

29.01 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 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 to comply with the above clause.

29.02 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.

(iii) Dangers of navigation, perils of the sea.

Note: Causes like power breakdowns/strikes, accidents etc do not fall under Force Majeure.

29.03 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.

29.04 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.

29.05 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.

29.06 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.
The Purchaser may terminate the contract after giving 7 (seven) days' notice if any of the following occurs:
i. Bidder fails to complete the execution of works within the approved schedule of works, terms and conditions.
ii. In case the Bidder commits any Act of Insolvency, or is adjudged insolvent
iii. Has abandoned the contract
iv. Has failed to commence work or has suspended the progress of works
v. Has failed to proceed with the works with due diligence and failed to make such due progress

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

29.08 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.

29.09 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 the failure to perform such obligations shall be due to an event of Force Majeure."

29.10 Severability
If any provision of this Agreement is or becomes invalid or unenforceable by the courts of any jurisdiction to which it is subject, such invalidity or unenforceability shall not prejudice the remaining provisions of this Agreement, which shall continue in full force and effect.

30.0 Transfer and Sub-Letting

30.01 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.

31.0 Recoveries

31.01 Whenever 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.

32.0 Waiver

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

33.0 Indemnification

33.01 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.

34.00 Termination for convenience of Purchaser

34.1 Purchaser at its sole discretion may terminate the contract by giving 30 days prior notice in writing or through email to the Supplier. Purchaser shall pay the Supplier for all the supplies/ services rendered till the actual date of contract termination against submission of invoice by the Supplier to that effect.

34.2 Payment of such compensation is the sole and exclusive remedy of the supplier for termination of this Agreement by Purchaser hereunder and the supplier shall not be entitled to, and hereby waives,
claims for lost profits and all other damages and expenses.

34.3 Supplier hereby agrees that substantiation for settlement of any claims submitted by supplier shall be complete and in sufficient detail to allow Purchaser's evaluation. Terminate all sub-contracts except those that have been/ to be assigned to the Purchaser all rights, titles and benefits of the Suppliers/Vendor as the case may be.

35.00 Documentation

35.01 The Bidder shall procure all equipment from BYPL-approved sources as per the attached specifications. The Bidders shall submit copies of Material/Type Test Certificates, O&M Manuals, and Approved & As-built drawings, related to various equipment (as applicable). The Bidder shall ensure strict compliance with the specifications and Field Quality Procedures issued by BYPL.

36.0 Transit Insurance

36.01 Transit Insurance shall be arranged by the Bidder.

36.02 DAMAGE / LOSS OF CARGO IN TRANSIT: The vendor shall be solely responsible for coordinating with the concerned insurance company for procuring insurance for material and/or Goods, processing claims lodgment and settlement. Notwithstanding the insurance cover, in case of loss/damage to material and/or Goods, in any manner and for any cause whatsoever, Vendor shall cause the damaged cargo to be replaced and delivered to the Purchaser with new material and/or Goods within 30 days of such loss/damage. The Vendor shall be solely responsible for all expenses in relation to the replacement and delivery in such circumstances.

37.0 Limitation of Liability

37.01 Except for willful misconduct or gross negligence, neither Party shall be liable to the other Party for loss of use of any Works, loss of profit, loss of any contract or any other indirect or consequential loss or damage which may be suffered by the other Party in connection with the Contract. The total liability of the Supplier to the Purchaser under the Contract shall not exceed the Contract Value. Except that this Clause shall not limit the liability of the Supplier:
(a) In cases of fraud, willful misconduct or illegal or unlawful acts, or
(b) In cases of acts or omissions of the Supplier that are contrary to the most elementary rules of diligence that a conscientious Supplier would have followed in similar circumstances.

38.0 Liability of Suppliers

38.1 Subject to the due discharge of its obligations under the Contract and except in case of gross negligence or willful misconduct on the part of the Supplier or on the part of any person acting on behalf of the Supplier, with respect to any loss or damage caused by the Supplier to the Purchaser's property or the Site, the Supplier shall not be liable to the Purchaser for the following:

(a) For any indirect or consequential loss or damage; and
(b) For any direct loss or damage that exceeds:
  (i) The total payments made and expected to be made to the Supplier under the Contract including reimbursements, if any; or
  (ii) The insurance claim proceeds that the Supplier may be entitled to receive from any insurance purchased by the Supplier to cover such a liability, whichever is higher.

38.2 This limitation of liability shall not affect the supplier's liability, if any, for damage to third-party property or injury or death of a person due to negligence of the Contractor or any Person or firm acting on behalf of the supplier in executing the order.

38.3 Notwithstanding anything contained in the Contract, the supplier shall not be liable for any gross negligence or willful misconduct on the part of the Purchaser or any of its affiliates, any vendor, or any party, other than Supplier and/or, its directors, officers, agents or representatives or its affiliates, or Sub-supplier, or the vendor or any third party engaged by it.

38.4 Notwithstanding anything contained in the Contract, including but not limited to approval by the Purchaser of any drawings, documents, vendor list, supply of information or data or the participation of the Purchaser in any meeting and/or discussion or otherwise, shall not absolve the Supplier from any of its liabilities or responsibilities arising in relation to or under the Contract.

39.0 Intellectual Property Rights and Royalties

39.1 The Supplier shall indemnify the Purchaser and the Purchaser's Representative from and against all claims and proceedings on account of infringement (or alleged infringement) of any patent rights, registered designs, copyright, design, trademark, trade name, know-how or other intellectual property rights (hereinafter collectively referred to as "**Intellectual Property Rights**") in respect of the Works, Supplier's Equipment, machines, Works method, Plant, Materials, or anything whatsoever required for the execution of the Works and from and against all claims, demands, proceedings, damages, costs, charges and expenses whatsoever in respect thereof or in relation thereto. In the event of an infringement of any Intellectual Property Rights of any third party as a result of the execution of the Works (or any part thereof) by the Supplier, the Supplier shall rectify, modify or replace, at its own cost, the Works, Plant or Materials or anything whatsoever required for the Works so that infringement ceases to exist or, in the alternative, the Supplier shall procure necessary rights/ licenses from the affected third party so that there is no infringement of Intellectual Property Rights.

39.2 The Supplier shall be promptly notified of any claim made against the Purchaser. The Supplier shall, at its cost, conduct negotiations for the settlement of such claim, and any litigation or arbitration that may arise from it. The Purchaser or the Purchaser's Representative shall not make any admission that might be prejudicial to the Supplier unless the Supplier has failed to take over the conduct of the negotiations, litigation or arbitration within a reasonable time after having been so requested. In the event of the Supplier failing to act at the Purchaser's Representative's notice, the Purchaser shall be at full liberty to deduct any such amount of pending claim from any amount due to the Supplier under the Contract or any other contract and the balance portion of claim shall be treated as debt due from the Supplier.

39.3 All Intellectual Property Rights in respect of any Plant, Materials, Drawings and Designs, plans, documents, specifications, data, materials, know-how, charts, information, etc., provided to the Supplier by the Purchaser pursuant to this Contract for the execution of the Works, belongs to and shall continue to belong to the Purchaser and the Supplier shall not have any rights in the same other than the limited right for its use for the purpose of execution of the Works.

39.4 Intellectual Property Rights in respect of any Plant, Materials, Drawings and Designs, plans, calculations, drawings, documents, know-how and information relating to the Works which are proprietary to the Supplier and/ or its third-party licensors ("**Supplier's IPR**") shall continue to vest with the Supplier and/ or its third-party licensors and the Supplier shall grant and/ or procure from its third party licensors, at its own cost, a worldwide, perpetual, royalty-free, non-exclusive license (along with the right to sub-license) to use and reproduce such Supplier's IPR for the use, operation, maintenance and repair of the Works.

39.5 If any patent, trademark, trade name, registered design or software is developed by the Supplier or its Sub-Supplier specifically for the execution of the Works, then all Intellectual Property Rights in respect of such design, trademark, trade name or software shall be the absolute property of the Purchaser and shall not be utilized or retained by the Supplier (or its Sub-Suppliers) for any purpose other than with the prior written consent of the Purchaser.

39.6 If the Supplier uses proprietary software (whether customized or off the shelf) for the purpose of storing or utilizing records in relation to the Works, the Supplier shall obtain at its own expense, the grant of a worldwide, royalty-free, perpetual licence or sublicence (including the right to sublicense) to use such software, in favour of the Purchaser provided that the use of such software under the licence or the sublicense may be restricted to use any such software only for the design, construction, reconstruction, manufacture, installation, completion, reinstatement, extension, repair and operation of the Works or any part thereof.

39.7 If any software is used by the Supplier for the execution of the Works over which the Supplier or a third party holds pre-existing title or other rights, the Supplier shall obtain for the Purchaser, a worldwide, royalty-free, perpetual license for the right to use and apply that software (together with any modifications, improvements and developments thereof).

40.0 Acceptance

40.01 Vendor confirms to have gone through the Policy of BYPL on legal and ethical code required to be followed by vendors encapsulated in the "Vendor Code of Conduct" displayed on the official website of BYPL (www.bsesdelhi.com) also, which shall be treated as a part of the contract/PO/WO.
The vendor undertakes that he shall adhere to the Vendor Code of Conduct and also agrees that any violation of the Vendor Code of Conduct shall be treated as breach of the contract/PO/WO.
In the event of any such breach, irrespective of whether it causes any loss/damage, Purchaser (BYPL) shall have the right to recover loss/damage from Vendor.
The Contractor/Vendor hereby indemnifies and agrees to keep indemnified the Purchaser (BYPL) against any claim/litigation arising out of any violation of Vendor Code of Conduct by the Contractor/Vendor or its officers, agents & representatives etc.

40.02 Acceptance of the CONTRACT implies and includes acceptance of all terms and conditions enumerated in the CONTRACT in the technical specification and drawings made available to Contractor consisting of general conditions, detailed scope of work, detailed technical specification, detailed equipment drawing and complete scope of work.

40.03 Contractor and Company contractual obligations are strictly limited to the terms set out in the CONTRACT. No amendments to the concluded CONTRACT shall be binding unless agreed to in writing for such amendment by both parties.

40.04 We expect your services and supplies to be aligned to our Vision, Mission and Values. Please refer to the following link to know about our Vision, Mission and Values; https://www.bsesdelhi.com/web/bypl/about-bses.

QUANTITY AND DELIVERY REQUIREMENTS

Sl. No.	BRPL SAP Code	Item Description	Specification	Total Qty.	Tentative Delivery Schedule	Destination
Part-A: (BRPL Supply)						
1	N/A	Supply of SIEM Solution with10000 EPS licenses (Provide price breakup separately in the block of 1000EPS)	VOLUME – III	**01** Lot	Delivery/completion within 06 months from the LOI/PO date.	BRPL Delhi Office(s)/ Site(s)
2	N/A	Supply of SOAR Solution (with 3 concurrent user license)		**01** Lot		
3	N/A	Supply of Network detection and response (NDR)		**01** Lot		
4	N/A	Hardware Appliance for SOC (Provide price breakup separately)		**01** Lot		
5	N/A	Workstation for SOC monitoring: (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)		**03** Nos		
6	N/A	27-inch FHD Monitor, IPS, 75 Hz, Bezel Less Design, AMD FreeSync, Flicker Free, HDMI, D-sub, 5 yrs warranty		**06** Nos		
7	N/A	85-inch industrial LED panel/screen for SOC with 2x2 screen splitter, 5 yrs warranty		**01** Nos		
Part – B: (BRPL - Installation, Commissioning and Testing)						
1		Installation, configuration and testing of SIEM, UEBA Solution		**01** Lot		
2		Installation, configuration and testing of SOAR Solution		**01** Lot		
3		Installation, configuration and testing of NDR Solution		**01** Lot		
4		Additional 2-year Warranty and Support for SIEM, UEBA, SOAR, NDR complete solution along with hardware and software (Optional)		**01** Lot		
Part-C: (BYPL Supply)						

1	N/A	Supply of SIEM Solution with10000 EPS licenses (Provide price breakup separately in block of 1000EPS)	VOLUME – III	**01** Lot	Delivery/completion within 06 months from the LOI/PO date.	BYPL Delhi Office(s)/ Site(s)
2	N/A	Supply of SOAR Solution (with 3 concurrent user license)		**01** Lot		
3	N/A	Supply of Network detection and response (NDR)		**01** Lot		
4	N/A	Hardware Appliance for SOC (Provide price breakup separately)		**01** Lot		
5	N/A	Workstation for SOC monitoring: (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)		**03** Nos		
6	N/A	27-inch FHD Monitor, IPS, 75 Hz, Bezel Less Design, AMD FreeSync, Flicker Free, HDMI, D-sub, 5 yrs warranty		**06** Nos		
7	N/A	85-inch industrial LED panel/screen for SOC with 2x2 screen splitter, 5 yrs warranty		**01** Nos		
Part – D (BYPL - Installation, Commissioning and Testing)						
1		Installation, configuration and testing of SIEM, UEBA Solution		**01** Lot		
2		Installation, configuration and testing of SOAR Solution		**01** Lot		
3		Installation, configuration and testing of NDR Solution		**01** Lot		
4		Additional 2-year Warranty and Support for SIEM, UEBA, SOAR, NDR complete solution along with hardware and software (Optional)		**01** Lot		
Part – E (BRPL - SOC Operations)						
1		1st year contract value for SOC Operations		Per annum		
2		2nd year contract value for SOC Operations		Per annum		
3		3rd year contract value for SOC Operations		Per annum		
Part – F (BYPL - SOC Operations)						

1		1st year contract value for SOC Operations		Per annum		
2		2nd year contract value for SOC Operations		Per annum		
3		3rd year contract value for SOC Operations		Per annum		

The delivery schedule shown above is tentative. PO(s) will be released as per the actual requirement. However, the supplier has to deliver the material within the delivery schedule provided.

Schemes may be executed in a phased manner.

ANNEXURE – 2.01

FORMAT OF PERFORMANCE BANK GUARANTEE
(To be executed on a Non-Judicial Stamp Paper of appropriate value)

This Guarantee made at ________ this [___] day of [_____] 20XX

1. WHEREAS M/s BSES Yamuna Power Limited, a Company incorporated under the provisions of Companies Act, 1956 having its Registered Office at Shaktikiran Building, Karkardoa, Delhi 110032, India hereinafter referred to as the " Owner ", (which expression shall unless repugnant to the context or meaning thereof include its successors, administrators, executors and assigns).

2. AND WHEREAS the Owner has entered into a contract for ____________(Please specify the nature of contract here) vide Contract No. ____________dated __________(hereinafter referred to as the "Contract") with M/s.________________, (hereinafter referred to as "the Supplier", which expression shall unless repugnant to the context or meaning thereof be deemed to mean and include each of their respective successors and assigns) for providing services on the terms and conditions as more particularly detailed therein.

3. AND WHEREAS as per clause ____of Conditions of Contract, the Suppliers are obliged to provide to the Owners an unconditional bank guarantee for an amount equivalent to ten percent (10%) of the total Contract Value for the timely completion and faithful and successful execution of the Contract from **[______________]** *pl. specify the name of Bank)* having its head/registered office at **[______________]** through its branch in ______*(pl. specify the name of Branch through which B.G is issued)* hereinafter referred to as "the Bank", (which expression shall unless it be repugnant to the context or meaning thereof be deemed to include its successors and permitted assigns).

4. NOW THEREFORE, in consideration inter alia of the Owner granting the Suppliers the Contract, the Bank hereby unconditionally and irrevocably guarantees and undertakes, on a written demand, to immediately pay to the Owner any amount so demanded (by way of one or more claims) not exceeding in the aggregate [Rs.]…………………*(in words)* without any demur, reservation, contest or protest and/or without reference to the Supplier and without the Owner needing to provide or show to the Bank, grounds or reasons or give any justification for such demand for the sum/s demanded.

5. The decision of the Owner to invoke this Guarantee and as to whether the Supplier has not performed its obligations under the Contract shall be binding on the Bank. The Bank acknowledges that any such demand by the Owner of the amounts payable by the Bank to the Owner shall be final, binding and conclusive evidence in respect of the amounts payable by the Supplier to the Owner. Any such demand made by the Owner on the Bank shall be conclusive and binding, notwithstanding any difference between the Owner and the Supplier or any dispute raised, invoked, threatened or pending before any court, tribunal, arbitrator or any other authority.

6. The Bank also agrees that the Owner at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor without proceeding against the Suppliers notwithstanding any other security or other guarantee that the Owner may have in relation to the Supplier's liabilities.

7. The Bank hereby waives the necessity for the Owner first demanding the aforesaid amounts or any part thereof from the Suppliers before making payment to the Owner and further also waives any right the Bank may have of first requiring the Owner to use its legal remedies against the Suppliers, before presenting any written demand to the Bank for payment under this Guarantee.

8. The Bank's obligations under this Guarantee shall not be reduced by reason of any partial performance of the Contract. The Bank's obligations shall not be reduced by any failure by the Owner to timely pay or perform any of its obligations under the Contract.

9. The Bank further unconditionally and unequivocally agrees with the Owner that the Owner shall be at liberty, without the Bank's consent and without affecting in any manner its rights and the Bank's obligation under this Guarantee, from time to time, to:

(i) vary and/or modify any of the terms and conditions of the Contract;

(ii) Forebear or enforce any of the rights exercisable by the Owner against the Suppliers under the terms and conditions of the Contract; or

(iii) Extend and/or postpone the time for performance of the obligations of the Suppliers under the Contract;

and the Bank shall not be relieved from its liability by reason of any such act or omission on the part of the Owner or any indulgence shown by the Owner to the Suppliers or any other reason whatsoever which under the law relating to sureties would, but for this provision, have the effect of relieving the Bank of its obligations under this Guarantee.

10. This Guarantee shall be a continuing bank guarantee and shall not be discharged by any change in the constitution or composition of the Suppliers, and this Guarantee shall not be affected or discharged by the liquidation, winding-up, bankruptcy, reorganization, dissolution or insolvency of the Suppliers or any of them or any other circumstances whatsoever.

11. This Guarantee shall be in addition to and not in substitution or in derogation of any other security held by the Owner to secure the performance of the obligations of the Suppliers under the Contract.

12. NOTWITHSTANDING anything herein above contained, the liability of the BANK under this Guarantee shall be restricted to ____________________*(insert an amount equal to ten percent (10%) of the Contract Value)* and this Guarantee shall be valid and enforceable and expire on ______________*(pl. specify date)* or unless a suit or action to enforce a claim under this Guarantee is filed against the Bank on or before the date of expiry.

13. On termination of this Guarantee, all rights under the said Guarantee shall be forfeited and the Bank shall be relieved and discharged from all liabilities hereunder.

14. The Bank undertakes not to revoke this Guarantee during its validity except with the prior written consent of the Owner and agrees that any change in the constitution of the Bank or the Suppliers shall not discharge our liability hereunder.

15. This Guarantee shall be governed by the laws of India. Any suit, action, or other proceeding arising out of, connected with, or related to this Guarantee or the subject matter hereof shall be subject to the exclusive jurisdiction of the courts of **Delhi,** India.

Dated this ………… day of ………….. …20XX at …………….

(Signature)

…………………………………………………………………
(Name)
…………………………………………………………………
(Designation with Bank Stamp)
Attorney as per
Power of Attorney No………………………………
Date……………………………………………………

ANNEXURE – 2.02

BYPL BANK DETAIL WITH IFSC CODE:

1. Name of the Bank:	Axis Bank Limited
2. Branch Name & Full Address:	C-58, Basement & Ground Floor, Preet Vihar, Main Vikas Marg, New Delhi 110092
3. Branch Code:	055
4. Bank Account No:	911030003596085
5. IFSC Code:	UTIB0000055
6. Swift Code:	AXISINBB055

ANNEXURE – 2.03

FORMAT OF WARRANTY/GUARANTEE CERTIFICATE

BSES YAMUNA POWER LIMITED Shaktikiran Building, Karkardooma, Delhi -110032.

Ref. Purchase Order No. :

Dear Sir,

We hereby confirm that the.................dispatched to BSES YAMUNA POWER LTD vide invoice no.......... DT..........is exactly of the same nature and description as per above mentioned Purchase Order.

We further confirm that we will replace/repair our........free of cost if any manufacturing defect during......months from the date of dispatch of material or......months from the date of commissioning whichever is earlier.

Vendor Name & Signature

ANNEXURE – 2.04

UNDERTAKING GST

The Vendor shall give an undertaking in the following words on each invoice in the absence of which tax payment as on the Vendor's invoice may be withheld.

"The tax component as mentioned in the invoice shall be deposited with the GST Department as per law by way of actual payment or by way of legal set off as per law. The turnover billed shall be duly declared in my GST returns a copy of which shall be filed with the Purchaser. Should the input tax credit to the Purchaser be denied by way of any lapse on the part of the Vendor, the same shall be paid on demand and in any case the Purchaser is authorized to deduct the tax equivalent amount from the amount payable to the Vendor"

ANNEXURE – 2.05

SUMMARY OF COMMERCIAL TERMS AND CONDITIONS

SL NO	PARTICULARS	CLAUSE AS PER TENDER	BIDDER'S CONFIRMATION
1	Validity	120 days from the date of submission of the bid	
2	Price basis	**"Firm"**, FOR Delhi store(s)/site(s) basis. Prices shall be inclusive of all taxes & duties, freight up to Delhi store(s)/site(s).	
3	Unloading	Unloading at stores/sites shall be in vendor's scope	
4	Transit insurance	Transit insurance in Bidder's scope	
5	Payment terms	Payment shall be done as per Clause No. 12 of NIT	
6	Delivery Schedule	Project shall be completed within 06 months from the LOI/PO date or completion as per the schedule.	
7	Defect Liability Period	**i)** Offered solution should be with onsite warranty and support. Bidder required to provide OEM warranty certificate. **ii)** 24x7, 4 hrs resolution, 5 years onsite Warranty (part and labor), support from OEM along with all patches for hardware and software	
8	Penalty for delay	1% (One) of the basic value (ex-works value) of undelivered units per week of delay or part thereof, subject to maximum of 10% (Ten) of the total basic value (ex-works value) of undelivered units.	
9	Performance Bank Guarantee	Performance Bank Guarantee within Twenty-eight (28) days, for an amount of 10% (Ten percent) of the Total Contract value. The Performance Bond shall be valid for a period of Sixty months (60) from the date of the commissioning or Sixty Six months (66) from the date of receipt of material (last consignment) at site/stores whichever is earlier plus 3 months towards claim period.	
10	Reverse Auction	In a bid to make our entire procurement process more fair and transparent, BYPL intends to use the reverse auctions through SAP-SRM tool as an integral part of the entire tendering process. All the bidders who are found as techno commercial qualified based on the tender requirements shall be eligible to participate in the reverse auction event.	

Seal of the Bidder:

Signature:

Name:

VOLUME – II

PRICE BID FORMAT

PRICE BID FORMAT FOR BRPL & BYPL

ALL PRICES IN INR (₹)

S. No.	DESCRIPTION OF GOODS	HSN CODE (8 Digit Mandatory)	UoM	QTY	UNIT BASIC PRICE INCL FREIGHT (₹)	UNIT GST & CESS AS APPLICABLE (CGST & SGST/ UTGST or IGST) (₹) **(C)**		UNIT LANDED RATE (All Inclusive) (₹)	TOTAL LANDED VALUE (₹)
				(A)	**(B)**	**%**	**AMT**	**(D=B+C)**	**(E=DXA)**
Part-A: (BRPL – Supply)									
1	Supply of SIEM Solution with10000 EPS licenses (Provide price breakup separately in the block of 1000EPS)		Lot	**01**					
2	Supply of SOAR Solution (with 3 concurrent user license)		Lot	**01**					
3	Supply of Network detection and response (NDR)		Lot	**01**					
4	Hardware Appliance for SOC (Provide price breakup separately)		Lot	**01**					
5	Workstation for SOC monitoring: (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)		Nos	**03**					
6	27-inch FHD Monitor, IPS, 75 Hz, Bezel Less Design, AMD FreeSync, Flicker Free, HDMI, D-sub, 5 yrs warranty		Nos	**06**					
7	85-inch industrial LED panel/screen for SOC with 2x2 screen splitter, 5 yrs warranty		Nos	**01**					
Total Amount Part - A									
Part – B: (BRPL - Installation, Commissioning and Testing)									
1	Installation, configuration and testing of SIEM, UEBA Solution		Lot	**01**					
2	Installation, configuration and testing of SOAR Solution		Lot	**01**					
3	Installation, configuration and testing of NDR Solution		Lot	**01**					

4	Additional 2-year Warranty and Support for SIEM, UEBA, SOAR, NDR complete solution along with hardware and software (Optional)		Lot	**01**					
Total Amount Part - B									
Part-C: (BYPL – Supply)									
1	Supply of SIEM Solution with10000 EPS licenses (Provide price breakup separately in block of 1000EPS)		Lot	**01**					
2	Supply of SOAR Solution (with 3 concurrent user license)		Lot	**01**					
3	Supply of Network detection and response (NDR)		Lot	**01**					
4	Hardware Appliance for SOC (Provide price breakup separately)		Lot	**01**					
5	Workstation for SOC monitoring: (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)		Nos	**03**					
6	27-inch FHD Monitor, IPS, 75 Hz, Bezel Less Design, AMD FreeSync, Flicker Free, HDMI, D-sub, 5 yrs warranty		Nos	**06**					
7	85-inch industrial LED panel/screen for SOC with 2x2 screen splitter, 5 yrs warranty		Nos	**01**					
Total Amount Part - C									
Part – D: (BYPL- Installation, Commissioning and Testing)									
1	Installation, configuration and testing of SIEM, UEBA Solution		Lot	**01**					
2	Installation, configuration and testing of SOAR Solution		Lot	**01**					
3	Installation, configuration and testing of NDR Solution		Lot	**01**					
4	Additional 2-year Warranty and Support for SIEM, UEBA, SOAR, NDR complete solution along with hardware and software (Optional)		Lot	**01**					
Total Amount Part - D									
Total Amount (A+B+C+D)									

Part – E: (BRPL - SOC Operations)									
1	1st year contract value for SOC Operations		Per annum	**01**					
2	2nd year contract value for SOC Operations		Per annum	**01**					
3	3rd year contract value for SOC Operations		Per annum	**01**					
Total Amount Part - E									
Part – F: (BYPL - SOC Operations)									
1	1st year contract value for SOC Operations		Per annum	**01**					
2	2nd year contract value for SOC Operations		Per annum	**01**					
3	3rd year contract value for SOC Operations		Per annum	**01**					
Total Amount Part - F									
TOTAL AMOUNT (E+F)									
GRAND TOTAL AMOUNT (Part A+B+C+D+E+F)									
In words									

NOTE: Cost of all tests as per technical specification is to be included. No separate charges will be paid.

The Un-priced bid should be marked as **"Quoted"** and be submitted with Part – A

We declare that the following are our quoted prices in INR for the entire package.

Date: Bidders Name:

Place: Bidders Address:

Signature: .... Designation: ....

Printed Name: .... Common Seal: ....

VOLUME – III

TECHNICAL SPECIFICATIONS

Technical Specification

Security Information and Event Management (SIEM) will be used to capture, correlate, monitor and alert all the incoming data to BRPL & BYPL 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 & BYPL to detect any anomalous behavior by analyzing the incoming traffic. Below table states the features of a SIEM tool as cited by BRPL & BYPL, 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 source.		
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, etc.		
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.		

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 13) Whitelist/Blacklist/Reference List		
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.		

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)		

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.		

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 integration.		
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		
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 • Unauthorized Bidder access to systems		

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 – STIX		
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 future.		
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		
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, 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		
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		

VOLUME – IV

SCOPE OF WORK

SCOPE OF WORK FOR SECURITY OPERATIONS CENTER (SOC) SETUP WITH OPERATIONS

1. SCOPE OF WORK

Request for Procurement (RFP) is to invited suitably experienced parties to build and operate Next Gen Security Operations Center (SoC) including supply and commission of technologies SIEM, SOAR, UEBA, NDR, Threat Intelligence, Threat Hunting, Incident Management along with operations of Security Operation Center. Supply, Installation and commissioning for SoC solution with 3 years warranty, support and operations for BSES RAJDHANI POWER LTD (BRPL) and BYPL YAMUNA POWER LTD (BYPL).

1.1. BRPL & BYPL 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 both respective companies BRPL & BYPL each.

1.3. The UEBA solution license should be for 4500 users for BRPL and 3000 users for BYPL.

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 & BYPL 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 & BYPL 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 & BYPL environment. Further, in case of any upgradation of current Hardware/OS/Database/application in BRPL & BYPL, 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 & BYPL'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 & BYPL, 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 & BYPL 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 & BYPL.

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

1.38. Bidders require to provide the POC as per the BRPL & BYPL request and requirement before finalization of the system. BRPL & BYPL reserve the rights to qualify or disqualify bidder solution based on PoC out come and deliverables. BRPL & BYPL 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 & BYPL 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.

SOC OPERATIONS SCOPE

2.1. SCOPE OF WORK

BRPL & BYPL 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 both companies BRPL & BYPL and needs to be run from respective 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 & BYPL. In case if L3 resource is required to visit BRPL & BYPL site for any incident handling same needs to be arranged onsite by bidder with no additional cost to BRPL & BYPL.

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

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

e) Bidder should have well qualified and experienced security professional's 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 & BYPL SOC. If resources are not certified bidder should ensure their certification within 3 months after deployment at BRPL & BYPL site.

g) Bidder should configure different dashboards as per BRPL & BYPL 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 BSES 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 & BYPL 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 & BYPL 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 & BYPL will provide the access of security devices like WAF, SIEM and SOAR etc installed at BRPL & BYPL 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 & BYPL before start of its services and comply with the BRPL & BYPL'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 & BYPL stakeholders • Coordinate and be present to discuss with BRPL & BYPL 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 & BYPL'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 & BYPL: within 24 hours • New use case creation as suggested by BRPL & BYPL: 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 & BYPL'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 & BYPL: • Daily reports: o Top attacker, attacks and attack targets, trends report o Top firewall ports access report (inbound/outbound) o Top signature triggered o Top account brute forced o Top systems infected o Top virus infection in the network o SIEM/monitoring tool performance report • Weekly reports: o Weekly security incidents status report o Daily device utilization report o Device availability report o Device: Incident, service request and change status report o Weekly threat advisory and vulnerability report o Top signature triggered o Top account brute forced o Top systems infected o Top virus infection in the network • Monthly reports: o Executive summary report for all the services o Monthly Security incident status report o Monthly security incident trend analysis o Monthly device availability report o 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 & BYPL 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 & BYPL on quarterly basis and BRPL & BYPL 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 & BYPL may initiate an interim review to check the performance and the obligations of the Agency. The BRPL & BYPL will conduct quarterly review of the services rendered by the Service Provider at mutually agreed schedules, dates and representatives from both the BRPL & BYPL 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

<b>Note: All incidents to be reported as per CERT-In, CEA or NCIIPC guidelines.</b></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
<b>Note: All incidents to be reported as per CERT-In, CEA or NCIIPC guidelines.</b></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 & BYPL 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 & BYPL 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.

2.6. TERMINATION PROCESS:

BRPL & BYPL reserve the rights to terminate the SOC operations contract on the basis of non-performance of the SOC service provider for continuous 3 months with a notice period of 3 months.

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 & BYPL 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 & BYPL.

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

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

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

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 optional additional two (2) years warranty and support needs to quote as per price bid (this will be optional).

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.