SOUTHERN POWER DISTRIBUTION COMPANY OF TELANGANA LIMITED
HYDERABAD

REQUEST FOR PROPOSAL

Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad.

RFP Bid Document No: CGM/IT/TSSPDCL/HYD/CYB-SECURITY/02/2021-22

The Chief General Manager/ IT
Southern Power Distribution Company
of Telangana Limited,

Phone: 040-23431276, 1287/74,
1st Floor, Corporate office,
Mint Compound, Hyderabad-500063.

Energy Saved is Energy Produced

SOUTHERN POWER DISTRIBUTION COMPANY OF TELANGANA LTD.

e-Procurement Tender Notice:

TSSPDCL intends to take up " **Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad ",** by calling Tenders on e-procurement platform. The details are as tabulated below.

Sl. No.	Name of the work	Specification No.	Date & time of downloading tender document	Closing Date & time for submission of bid
1.	Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad	CGM/IT/TSSPDCL/HYD/CYB-SECURITY/02/2021-22	31.07.2021 from 11:00 hrs to 12.08.2021 Up to 17:00 hrs	13.08.2021 at 12:00 hrs

For further details regarding detailed tender notification, specifications and digital certificate please visit **www.eprocurement.telangana.gov.in, www.tender.telangana.gov.in & www.tssouthernpower.com .**

Phone: 040-23431276, 1287, 1274.

CHIEF GENERAL MANAGER/IT

SOUTHERN POWER DISTRIBUTION COMPANY OF TELANGANA LTD.
Hyderabad

REQUEST FOR PROPOSAL (RFP)

Tender specification No. CGM/IT/TSSPDCL/HYD/CYB-SECURITY/02/2021-221.

TSSPDCL invites bids from eligible bidders for Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad as defined in the bid document.

2. Brief description of "the works" is as follows:

Sub-Project No.	Name of the work	Estimated cost (Rs. in Lakh)	Project implementation period	Bid security (2%) (Rs. in Lakh)
CGM/IT/TSSPDCL/HYD/SEC AUDIT/02/2021-22	Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad.	40.0	6 months	80,000/-

3. All the interested bidders may visit **www.eprocurement.telangana.gov.in** **www.tender.telangana.gov.in** & **www.tssouthernpower.com** to view and download the tender documents free-of-cost from **31.07.2021, 11:00 Hrs. to 13.08.2021, 12.00 Hrs**.

4. Those who are interested to submit bids will have to register in the above-mentioned site and also have to obtain Digital Certificates. The details and procedure for obtaining digital certificate are mentioned in the website or contact the helpdesk of the site.

CONTENTS OF TENDER SCHEDULE

RFP Bid Document No: CGM/IT/TSSPDCL/HYD/CYB-SECURITY/02/2021-22

INDEX

SECTION-I

Notice Inviting Tender (NIT)

RFP Bid Document No: CGM/IT/TSSPDCL/HYD/CYB-SECURITY/02/2021-22

S.No	Description	Details
1	Department Name	Southern Power Distribution Company of Telangana Limited
2	Office Address	**Chief General Manager/IT,** **1st Floor, Corporate Office,** **Mint Compound,** **HYDERABAD**
3	RFP/Bid Number	**CGM/IT/TSSPDCL/HYD/CYB-SECURITY/02/2021-22**
4	Tender Subject	Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad.
5	Estimate Contract value	**Rs.40.0 Lakhs** (Rupees Forty Lakhs only)
5 (a)	Type of quotation	**Item-wise Rates** **(The bidder has to quote as Item- wise rates in Financial bid)**
6	Period of Work	Within 6 months from the date of LOA.
7	Tender Type	Open
8	Tender Category	Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad.
9	Bid Security (INR)	**Rs.80,000/- (Rupees Eighty Thousand only)**
10	Bid Security Payable to	In the form of DD in favor of Pay Officer/TSSPDCL/Hyderabad **(or) BG from Nationalized/Scheduled bank as per Annexure-VIII**
11	Schedule Sale opening date	**31.07.2021 at 11:00 hrs**
12	Pre-Bid Meeting date	**--**
13	Schedule Sale Closing Date	**12.08.2021 at 17:00 Hrs.**
14	Bid Submission Closing Date	**13.08.2021 at 12:00 Hrs.**
15	Technical Bid Opening Date	**13.08.2021 at 15:00 Hrs.**
16	Price Bid Opening Date (Financial Bid Stage)	**20.08.2021 at 12:00 Hrs.**
17	Place of Tender Opening	Corporate Office, TSSPDCL, Hyderabad.
18	Officer Inviting Bids	Chief General Manager/IT
19	Address & Email.ID	**Chief General Manager/IT,** **1st Floor, Corporate Office,** **Mint Compound,** **HYDERABAD** cgmit@tssouthernpower.com
20	Contact Details	**040-23431276,1287, 1274**

21	Eligibility Criteria	**As per the Qualification requirements mentioned in Section-IV** Even though the bidder meets the above qualifying criteria, they are subject to be disqualified if they have made misleading or false representations in the forms statements and attachments submitted in proof of qualification requirements and/ or record of poor performance such as not properly completing the contract, inordinate delays in works completion, litigation history or financial failure etc. Notwithstanding anything stated above, TSSPDCL reserves the right to assess bidder's capability and capacity to perform the contract should circumstances warrant such as assessment in the overall interest of the Department.
22	Procedure for Bid Submission	**Bids shall be submitted online** on www.eprocurement.telangana.gov.in, www.tender.telangana.gov.in platform. The Technical Bid and Price Bid(Commercial Bid) shall be quoted separately. Quoted price should not be mentioned anywhere (in any format) in the Technical Bid (Both Online or Offline). The Technical bid shall be submitted in online & Offline. The Price bids shall be submitted online only in commercial stage. 1. The participating bidders in the tender should register themselves free of cost on e-procurement platform in the website www.eprocurement.telangana.gov.in, www.tender.telangana.gov.in. 2. Bidders can log-in to e-procurement platform in secure mode only by signing with the Digital certificates. 3. The bidders who are desirous of participating in Tender shall submit their technical bids, price bids as per the standard formats available at the www.tssouthernpower.com. 4. The bidders should submit the following documents in support of technical bids. The bidders shall sign on all the statements, documents certificates, owning responsibility for their correctness/authenticity: a) Bid Security should be furnished i) In the form of DD in favour of Pay Officer/TSSPDCL/ Hyderabad (or) Alternatively, BG from Nationalized/Scheduled bank in favor of Chief General Manager/IT/TSSPDCL/ Hyderabad as per Annexure-VIII enclosed. ii) If exempted give details of Bid Security Exemption in case of Govt. firms. b) Financial Turnover certified by CA as per RBI guidelines, as mentioned in Eligibility criteria. c) Duly filled and signed Proforma as per Annexure-X. The copies of certificates, documents, original Demand Drafts in respect of Bid Security are to be submitted by the bidder to the Chief General Manager/IT/TSSPDCL, so as to reach before the date and time of opening of the technical bid. Failure to furnish any of the documents, certificates, before the date and time of opening of technical bid will entail in rejection of the bid. The Department shall not hold any risk on account of postal delay. Similarly, if any of the certificates, documents, etc., furnished by the tenderer are found to be false/fabricated/bogus, the bidder will be disqualified, blacklisted, action will be initiated as deemed fit and the Bid Security will be forfeited.
23	Rights reserved with the Department	TSSPDCL reserves the right to accept or reject any or all of the tenders received without assigning any reasons therefore. TSSPDCL also reserves the right to split the tender and place contract on more than one bidder at its discretion.
24	General Terms & Conditions	As per tender documents.

Chief General Manager/IT,
1st Floor, Corporate Office,
Mint Compound,HYDERABAD-63.

SECTION-II

INSTRUCTIONS TO BIDDERS

A. General

TSSPDCL is a Power distribution utility engaged in the business of distributing power to its consumers. TSSPDCL intends to Implement Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad and conduct Security audit of its IT Systems to identify specific exploitable vulnerabilities and to expose potential entryways to vital or sensitive data.

At present, the TSSPDCL applications are centrally hosted at Data Center located in premises of Corporate Office, Hyderabad which includes SAP ERP System and In-house developed applications. The Call Centre & SCADA System is located at TSSPDCL SCADA office at G.T.S.Colony, Erragadda, Hyderabad.

The Security consultant has to perform security audit of applications from the internal and external perspective.

1. SCOPE OF BID

The TSSPDCL (referred to as Customer/Employer in this document) invites bids for "Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad.".

2 SCOPE OF WORK

2.1 TSSPDCL through this RFP intends to implement ISMS/ISO27001:2013(or latest) and conduct Security Audit of IT Systems of TSSPDCL through a CERT-IN Empanelled Security Auditing Agency. The audit of the IT Systems applications shall be done by the Auditing Agency in the premises of TSSPDCL Offices, at Hyderabad.

2.2 The Auditor should prepare all the documentation for ISMS based on the Discom policies and provide ISO27001:2013(or latest) certification for the TSSPDCL Data Centre located at Mint Compound, Hyderabad and SCADA Centre at Erragadda, Hyderabad and its related equipment. in accordance with Annexure-XI .

2.3 The Auditor should prepare a Cyber Crisis Management Plan in accordance with Annexure-XI.

2.4 Mock drill exercises shall be conducted for identifying the shortcoming(s) and to improve preparedness to handle cyber breach/incidents

2.5 The Auditor should provide the recommendations for overcoming and mitigating the identified vulnerabilities along with recommendations for the possible security infrastructure (like the Firewall, etc.) needed at TSSPDCL Data Center and SCADA Center. Accordingly, the Auditor shall deploy its team in TSSPDCL for conducting the audit as and when intimated by TSSPDCL to Auditor in writing / e-mail.

2.6 The Auditor shall estimate their efforts and team size in line with the project requirements and timelines as provided in this RFP and deploy the required team accordingly. TSSPDCL shall only provide the seating space to the team of Auditor. Auditor will provide detailed report on implementable step by step solution suggested for fixing of vulnerabilities found within existing applications and will provide onsite support to TSSPDCL.

The Detailed Scope of Work is mentioned in **Section -V** of this Tender document.

3 ELIGIBILITY CRITERIA:

The bidder should meet the Qualification requirements as mentioned in **Section-IV** of the bid document

B. BIDDING DOCUMENTS

4. CONTENT OF BIDDING DOCUMENTS:

4.1 The Schedule of requirement, bidding procedures, and contract terms are prescribed in the bidding documents as listed below:

a. Notice Inviting Bids.
b. Instruction to Bidders
c. General Terms and Conditions of Contract.
d. Qualification Requirements.
e. Scope of work
f. Payment & Penalty
g. Sample Forms & Annexure's

- Bid Form and Price Schedules
- Bid Security Form
- Contract Form
- Performance Security form
- Manufacturers' Authorization form
- Performance Statement
- Details to be furnished by the Manufacturer (Format-A)
- Schedule of Deviations (Technical & Commercial)
- Financial bid format

4.2 The Bidder is expected to examine all instructions, forms, terms and technical specifications in the bidding documents. Failure to furnish all information required by the bidding documents or to submit a bid not substantially responsive to the bidding documents in every respect will be at Bidder's risk and may result in the rejection of its bid.

5. CLARIFICATION OF BIDDING DOCUMENTS:

A prospective bidder requiring any clarification of the bidding documents may notify the Employer in writing or by e-mail (hereinafter "cable" includes telegram) at the Employer's address indicated in the invitation to bid. The Employer will respond to any request for clarification, which he received earlier than **15 days** prior to the deadline for submission of bids. Copies of the Employer's response will be forwarded to all Employers of the bidding documents, including a description of the enquiry but without identifying its source **"Annexure-VI"**

6. AMENDEMENT OF BIDDING DOCUMENTS

6.1 Before the deadline for submission of bids, the Employer may modify the Bidding documents by issuing addenda will be posted in www.tssouthernpower.com.

6.2 Any addendum thus issued shall be part of the bidding documents and shall be uploaded in www.tssouthernpower.com

6.3 To give prospective bidder reasonable time in which to take an addendum into account in preparing their bids, the Employer shall extend as necessary the deadline for submission of bids.

C. PREPARATION OF BIDS

7. LANGUAGE OF THE BID

All documents relating to the bid shall be in the English language

8. DOCUMENTS COMPRISING THE BID

The bid submitted by bidder shall be of double packet comprising of the following.

(a) **Technical Bid**: Technical bid consists of bid security and qualification information with necessary supporting documents.

(b) **Price Bid**: Price bid consists of the Commercial Template and bid document.

9. BID PRICES:

a. All the prices would be quoted only in Indian Rupees (INR) currency
b. Prices/ Rates shall be written both in words and in figures. There would not be errors and/ or over-writings. Corrections/ alterations, if any, would be made clearly and initialed with date.
c. The prices and discounts quoted by the Bidder in the Price Schedule/ Commercial/ Financial Bid shall conform to the requirements specified therein.
d. All Bidders' service categories in the Financial Bid must be listed and priced separately. If a Price Schedule shows items listed but not priced, their prices shall be assumed to be included in the prices of other items. Items not listed in the Price Schedule shall be assumed not to be included in the Bid, and provided that the Bid is substantially responsive, the corresponding adjustment shall be applied in accordance with the provisions of bid document.
e. The price to be quoted in the Bid Submission Sheet shall be the total price of the Bid including any discounts offered.
f. Prices quoted by the Bidder shall be fixed during currency of the Contract and not subject to variation on any account. A Bid submitted with an adjustable price quotation shall be treated as nonresponsive and shall be rejected.
g. Unless otherwise indicated in the bid document, prices quoted shall correspond to100% of the services to be provided.

10. Taxes & Duties

a. The bidder shall be familiar with the tax laws of the country, unless otherwise specified in the contract.
b. GST as applicable to services that are not directly provided to the employer such as transport, insurance etc. must be included in the unit price only.
c. The unit rate arrived by the Bidder must be exclusive of all taxes.
d. The 1% Workers' Welfare Cess included in the rate will be recovered from Contractor bills for remittance to the Government
e. The applicability of all taxes and appropriate rates must be ascertained by the Bidder before submitting his bid
f. The prices shall be firm during currency of the contract.
g. The variation in taxes and duties if any is not applicable for bought out items / material.
h. Beyond the date of schedule contract agreement period any increase in statutory levies shall be to the account of bidder.

11. CURRENCIES OF BID AND PAYMENT

a. The unit rates and the prices shall be quoted by the bidder entirely in Indian Rupees.
b. The BIDDER shall raise invoices for services rendered in triplicate as per payment schedule to the respective controlling officers, who will forward the bills to the paying authority through the Chief General Manager/IT. The payment for above work will be made by Pay Officer, of the respective Customer after verification of bills by the CGM(IT) designated for the purpose.

12. BID VALIDITY

a. Bids shall remain valid for a period not less than **90 days** after the deadline date of bid submission specified. A bid valid for a shorter period shall be rejected by the Employer as non-responsive.
b. In exceptional circumstances, prior to expiry of the original time limit, the Employer may request that the bidders may extend the period of validity for a specified additional period. The request and the bidder's responses shall be made in writing or by cable. A bidder may refuse the request without forfeiting his bid security. A bidder agreeing to the request will not be required or permitted to modify his bid, but will be required to extend the validity of his bid security for a period of the extension, under this Section in all respects.

13. BID SECURITY

a. The Bidder shall furnish, as part of its bid, a Bid Security of **Rs. 80,000/- (Rupees Eighty Thousand only).** This amount should be paid by way of a crossed demand

draft drawn on any scheduled bank in favor of the Pay Officer, TSSPDCL and payable at headquarters of the **Employer**. The crossed DD should invariably be furnished along with the bids. Alternatively, the bidders may furnish a **B.G. from any nationalized/scheduled bank** in original in lieu of DD as per the proforma attached. Fax / photocopies of the bid security will not be accepted and will be rejected.

b. The fact of having enclosed bid security by DD/BG along with the bid should be clearly super scribed on the bid envelope.
c. Submission of BID SECURITY by way of cheque, cash, money order, call deposit will not be accepted and will be considered as disqualification.
d. Payment of BID SECURITY will be waived at the discretion of the Customer in the case of fully owned Government undertaking of the Central or State Government. Such undertakings should immediately apply and obtain exemption before submitting their Bids. They need only refer to the details of such exemption in their Bids. Exemption accorded by any organization other than respective Customers will not be considered.
e. Requests for exemption from payment of BID SECURITY will not be entertained in any other case.
f. Any bid not secured as above will be rejected by the Employer.
g. Unsuccessful Bidders' Bid Security will be discharged or returned as promptly as possible, but not later than thirty (30) days after the expiry of the period of bid validity prescribed by the Employer.
h. The successful Bidder's Bid Security will be discharged upon the Bidder signing the contract.
i. **The Bid Security may be forfeited:**

A. if a Bidder:

i) Withdraws its bid or alters its prices during the period of bid validity specified by the Bidder on the Bid Form, or

ii) Offers post Bid rebates, revisions or deviations in quoted prices and / or conditions or any such offers which will give a benefit to the Bidder over others will not only be rejected outright but the original Bid itself will get disqualified on this account and the Bidder's BID SECURITY will be forfeited.

B. In the case of a successful Bidder, if the Bidder fails:
   i) To sign the contract in accordance with Clause No.30
   ii) To furnish performance security in accordance with Clause No.31

j. In cases where the Bid Cover Contains superscription of having furnished Bid Security by way of DD/BG but if the same is not found within, such Bids will be rejected and bidder will run the risk of being banned.

Note: -The bidder shall furnish required Bid Security amount and validity (The validity of the bank guarantee shall be up to bid validity +45 days from the date of tender opening) as per specification. If the bidder fails to furnish bid security amount and bid validity as stipulated in the specification, such tender bid will not be considered for further evaluation

k. No interest will be paid by the Customers on the Bid Security deposited.
l. If the lowest bidder backs out at the time of agreement, penalty of forfeiture of EMD will be imposed and business of the agency will be suspended for one year with all the Departments in Telangana.

14. ALTERNATIVE PROPOSALS BY BIDDERS

Bidder shall submit offers that comply exactly with the requirements of the bidding documents, including the basic technical design as indicated in the drawings and specifications. **Alternative offers with any conditions will not be considered.**

15. FORMAT AND SIGNING OF PRICE BID

The Bidder shall furnish information as described in the form of Bid on commissions or gratuities, if any, paid or to be paid to agents relating to the Bid and to contract execution if the Bidder is awarded the contract.

D. SUBMISSION OF BIDS

16. Submission, Sealing and Marking of Bids.

16.1 The Bidders are requested to submit their bid in two parts as under:

i) The Part – I consists the following documents

S. No.	Document Type	Document Format
Fee Details (In sealed cover-1)		
1	Earnest Money Deposit	Demand draft/Bank Guarantee/Valid exemption certificate
Pre-Qualification Documents (In sealed cover-1)		
1.	Eligibility Criteria References	As per format given in **Annexure II**
2.	Bidder's Authorization Certificate	As per format given in **Annexure III**
3.	Self-declaration – no blacklisting	As per format given in **Annexure IV**
4.	All the documents mentioned in the "Eligibility Criteria" in support of the eligibility.	Requisite supporting documents meeting eligibility criteria as specified in Section-I
Technical Bid Documents ((In sealed cover-1)		
1.	Technical Proposal Submission form	On Bidder's original letter head and as per format provided in **Annexure I-A** and duly signed by authorized signatory as per **Annexure III**
2.	Bidder's organization Profile	Brief organization profile of the Bidder
3.	Firm's references to showcase relevant experience along with necessary proofs and credentials	As per **Annexure I-B**
4.	Details of Team composition, qualification and experience	As per **Annexure I-C**
5.	Signed and latest CVs of proposed Bidders format	As per **Annexure I-D**

ii) The Part-II : Price Bid – containing Prices

iii) The Part-I of tender should be furnished in a sealed cover super scribing tender enquiry number, name of material, name of the bidder and date of tender opening. The Technical Bid and Price Bid(Commercial Bid) shall be quoted separately. Quoted price should not be mentioned anywhere (in any format) in the Technical Bid(Both Online or Offline).
The Technical bid shall be submitted in online & Offline.
The Price bids shall be submitted online only in commercial stage.

iv) Part-I of the bid will be opened on the due date of tender opening. In case the bidders have been granted Bid Security exemption, documentary evidence for the same must be furnished. The firms whose Bid Security is not received as specified in the tender document, the price bids will not be opened and their bids will be rejected summarily.

v) The price bids of only those bidders whose technical bids, on examination, are determined to be technically and commercially acceptable and meeting the specified Qualification Criteria will be opened at a later date.

Sealing and Marking of Bids

16.2 The Bidder shall seal the original in separate envelope, duly marking envelope as "ORIGINAL".

16.3 The inner and outer envelopes will:

Be addressed to the Employer (TSSPDCL).

16.4 The sealed cover as well as the outer envelope should be super scribed as follows:

a. Bid Enquiry No.
b. Payment of Bid Security
   i) If paid, give details: D.D. No. Date:
   ii) If not paid or exempted, give details.

c. Whether 120 days validity offered…….YES / NO
d. Whether the quotation is made accepting Payment terms clause …. YES/NO
e. Whether the bid is quoted in two parts (clause 21.1)…. (YES/NO)

16.5 Bids not super scribed as above are liable to be rejected.

16.6 The Bidder shall invariably complete the Bid in full. Details to be furnished by the bidder and Schedule of Prices attached to the specification and enclose the same to the bid without fail.

16.7 The bids shall be in bound volumes (With the documents in the volume not detachable). All pages of the bid except in-amended printed literature shall be initiated by the person/persons signing the bid. The page number shall be referred in Index. All pages including literature, type test reports of the bid shall be numbered and the page numbers shall be continuous. Soft copy of the technical and commercial bids and designs with drawings shall be given in Floppy disc/ CD also. Summary sheet in the given format on the top of the bid duly signed and sealed by the bidder.

16.8 The time of actual receipt in the office only will count for the acceptance of the bid and either the date of bid, date stamp of post office or date stamp of any other office will not count. The TSSPDCL will not be responsible for any postal or any other transit delays.

16.9 Telegraphic quotations will not be entertained under any circumstances. Clarification, amplifications, and/or any other correspondence from the Bidder subsequent to the opening of bid will not be entertained. The Bidders are advised to ensure that their bids are sent in complete shape at the first instance itself.

16.10 The inner envelopes shall also indicate the name and address of the Bidder to enable the bid to be returned unopened in case it is declared "late".

16.11 If the outer envelope is not sealed and marked as required above, the Employer will assume no responsibility for the bid's misplacement or premature opening.

17. Deadline for Submission of Bids.

17.1 Bids together with modifications if any, or other withdrawals must be received by the Employer not later than the deadline for submission of bids specified in the Salient features of the Bid**.**

17.2 The Employer may, at its discretion, extend this deadline for the submission of bids by amending the bidding documents in which case all rights and obligations of the Employer and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

18. Late Bids

18.1 Any bid received by the Employer after the deadline for submission of bids prescribed by the Employer will be rejected and returned unopened to the Bidder.

18.2 Modification and Withdrawal of Bids.

The Bidder may modify or withdraw its bid after the bid's submission, provided that written notice of the modification, including substitution or withdrawal of the bids, is received by the Employer prior to the deadline prescribed for submission of bids.

The Bidder's modification or withdrawal notice will be prepared, sealed, marked, and dispatched. A withdrawal notice may also be sent by cable, but followed by a signed confirmation copy, postmarked not later than the deadline for submission of bids. No bid may be modified after the deadline for submission of bids.

No bid may be withdrawn in the interval between the deadline for submission of bids and the expiration of the period of bid validity specified. Withdrawal of a bid during this interval may result in the forfeiture of its Bid Security.

E. BID OPENING AND EVALUATION

19. BID OPENING

The Employer will open all the Technical Bids received in time. In the event of the specified date of Bid opening being declared a holiday for the Employer, the Technical Bids will be opened at the appointed time and location on the next working day and evaluation of the Technical bid will be taken up.

19.1 Bid Evaluation Methodology and Selection of Projects

19.2 Bid Evaluation Methodology

The evaluation process comprises the following two steps:

A. 1st Step – Prequalification (PQ)

B. 2st Step – Technical evaluation

C. 3rd Step – Financial Bid evaluation

A. 1st step: – Prequalification (PQ)

The Bidder shall submit the EMD in a separate Envelope. The same shall be submitted to the Authorised Representative before the Bid Deadline.

The Bidder shall submit original documents pertaining to EMD. Bids not accompanied by EMD as per the terms of the RFP shall be summarily rejected and no further evaluation will be carried out in respect of such Bids/Bidders

Any of the following conditions shall cause the Bid to be "Non-responsive":

i) Non submission of EMD in acceptable form/amount along with the response to RFP

ii) Bids not received by the Bid Deadline.

B. 2nd step: – Technical Bid Evaluation

The Employer will open all the Technical Bids received in time. In the event of the specified date of Bid opening being declared a holiday for the Employer, the Technical Bids will be opened at the appointed time and location on the next working day and evaluation of the Technical bid will be taken up.

C. 3rd Step – Financial Bid evaluation

The Employer will award the Contract to the Bidder whose Bid has been determined to be substantially responsive to the Bidding documents and who has offered the lowest evaluated Bid Price, provided that such Bidder has been determined to be (a) eligible in accordance with the provisions of qualified in accordance with the provisions of section 1.

20. 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 until the award to the successful Bidder has been announced. Any effort by a Bidder to influence the Employer's processing of Bids or award decisions may result in the rejection of his Bid.

21. CLARIFICATION OF BIDS

21.1 To assist in the examination, evaluation, and comparison of Bids, the Employer may, at his discretion, ask any Bidder for clarification of his Bid, including breakdowns of unit rates. The request for clarification and the responses shall be in writing or by e-mail, but no change in the price or substance of the Bid shall be sought, offered, or permitted.

21.2 Subject to above, no Bidder shall contact the Employer on any matter relating to its bid from the time of the bidding opening to the time of the contract is awarded. If the Bidder wishes to bring additional information to the notice of the Employer, he should do so in writing.

21.3 Any effort by the Bidder to influence the Employer in the Employer's bid evaluation, bid comparison or contract award decisions may result in the rejection of the Bidder's bid.

22. EXAMINATION OF BIDS AND DETERMINATION OF RESPONSIVENESS

22.1 Prior to the detailed evaluation of Bids, the Employer will determine whether each Bid (a) meets the eligibility criteria defined under this section (b) has been properly

signed; (c) is accompanied by the required securities and; (d) is substantially responsive to the requirements of the Bidding documents.

22.2 A substantially responsive Bid is one which conforms to all the terms, conditions, and specifications of the Bidding documents, without material deviation or reservation. A material deviation or reservation is one (a) which affects in any substantial way the scope, quality, or performance of the Works (b) which limits in any substantial way, inconsistent with the Bidding documents, the Employer's rights or the Bidder's obligations under the Contract, or (c) whose rectification would affect unfairly the competitive position of other Bidders presenting substantially responsive Bids.

22.3 If a Bid is not substantially responsive, it will be rejected by the Employer, and may not subsequently be made responsive by correction or withdrawal of the non-confirming deviation or reservation.

23 VALUATION AND COMPARISION OF BIDS

23.1 The Employer will evaluate and compare only the Bids determined to be substantially responsive.

23.2 The Employer reserves the right to accept or reject any variation, deviation, or alternative offer. Variation, deviations, and alternative offers and other factors which are in excess of the requirements of the Bidding documents or otherwise result in unsolicited benefits for the Employer shall not be taken into account in Bid evaluation.

23.3 If the Bid of the successful Bidder is seriously unbalanced in relation to the Engineer's estimate of the cost of work to be performed under the contract, the Employer may require the Bidder to produce detailed price analysis for any or all items of the Bill of Quantities, to demonstrate the internal consistency of those prices with the construction methods and schedule proposed. After evaluation of the price analyses, the Employer may require that the amount of the performance security set forth under this Section be increased at the expense of the successful Bidder to a level sufficient to protect the Employer against financial loss in the event of default of the successful Bidder under the Contract.

24 Conflict of Interest

I. TSSPDCL considers a conflict of interest to be a situation in which a party has interests that could improperly influence that party' performance of official duties responsibilities, contractual obligations, or compliance with applicable laws and regulations. In pursuance of TSSPDCL's procurement ethics, the bidders, Bidders, and contractor sunder contracts, observe the highest standard of ethics, TSSPDCL will take appropriate actions against the bidder, if it determines that a conflict of interest has flawed the integrity of any procurement process. Consequently all bidders found to have a conflict of interest shall be disqualified.

II. It may be considered to be in a conflict of interest with one or more parties in the bidding process if

a) They have controlling shareholders in common; or
b) It receives or have received any direct or indirect subsidy from any of them; or
c) They have the same legal representative for purposes of the Bid; or
d) They have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about or influence on the Bid of another Bidder, or influence the decisions of the tendering authority regarding this bidding process.

25 Disqualification

Tendering authority may at its sole discretion and at any time during the processing of bid, disqualify any bidder /bid from the bid process if the bidder:-

a. Has not submitted the bid in accordance with the bidding document.
b. Does not meet the minimum eligibility criteria as mentioned in the bidding document.

c. During validity of the bid or its extended period, if any, increases his quoted prices.
d. Has imposed conditions in his bid.
e. Has made misleading or false representations in the forms, statements and attachments
f. submitted in proof of the eligibility requirements.
g. Has submitted the bid after due date and time.
h. Has offered lesser number of resources than that is required for a service category.
i. Is found to have a record of poor performance such as a abandoning work, not properly completing the contract, inordinately delaying completion, being involved in litigation or financial failures, etc.
j. Has submitted bid which is not accompanied by required documentation and EMD.
k. Has failed to provide clarifications related thereto, when sought.
l. Has submitted more than one bid. This will cause disqualification of all bids submitted by such bidders including for feature of the EMD.
m. Who is found to canvass, influence or attempt to influence in any manner for the qualification or selection process, including without limitation, by offering bribes or other illegal gratification shall bed is qualified from the process at any stage.

26. Evaluation of Financial Bids

The Employer will award the Contract to the Bidder whose Bid has been determined to be substantially responsive to the Bidding documents and who has offered the lowest evaluated Bid Price, provided that such Bidder has been determined to be (a) eligible in accordance with the provisions of qualified in accordance with the provisions of section 1.

27. Negotiations

a. As a general rule, negotiations after opening of bids would be discouraged. However, negotiations may be under taken in exceptional circumstances, such as when the quoted rates have wide variations and are much higher than the market rates prevailing at the time of opening of bids.
b. Negotiations shall not make original offer of the bidder ineffective.
c. In case the lowest/best bidder does not reduce his rates in response to negotiations or the rates so reduced are still considered to be higher, the tendering authority may decide to make a written counter offer to the lowest/best bidder. If the lowest/best bidder does not accept the counter offer given by the tendering authority, the tendering authority may recommend for rejection of the bid or may repeat the process to make the same counter offer to second lowest/best bidder and soon to third, fourth lowest/best bidder, etc. till any bidder accepts it.

F. AWARD OF CONTRACT

28. AWARD CRITERIA

28.1 The Employer will award the Contract to the Bidder whose Bid has been determined to be substantially responsive to the Bidding documents and who has offered the lowest evaluated Bid Price, provided that such Bidder has been determined to be (a) eligible and (b) qualified.

29. EMPLOYER'S RIGHT TO ACCEPT OR REJECT ANY BID / ALL BIDS

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

30. NOTIFICATION OF AWARD AND SIGNING OF AGREEMENT

30.1 The Bidder whose Bid has been accepted will be notified of the award by the Employer prior to expiration of Bid validity period by writing or by e-mail by registered letter. This letter (hereinafter in the Conditions of Contract called the "**Letter of Acceptance**") will state the sum that the Employer will pay the Contractor in consideration of the execution, completion, and maintenance of the works by the Contractor as prescribed by the Contract (hereinafter and in the Contract called the "**Contract Price**").

30.2 The notification of award will constitute the formation of the Contract, subject only to the furnishing of a Performance Security to the Customers.

30.3 The Agreement will incorporate all agreements between the Employer and the successful Bidder. The agreement will be signed by the successful bidder and the Customer authorized Signatory **within 28 days** after receipt of the Letter of Acceptance (Notification of Award) by the successful Bidder.

30.4 The successful Bidder must produce GSTIN (Goods and Service Tax Identification Number) before the issue of Letter of Acceptance

31 PERFORMANCE SECURITY

31.1 Within **21 days** of receipt of the Letter of Acceptance, the Successful Bidder shall deliver to the Customers, a Performance Security in any of the forms given below for an amount equivalent to **5% of the Contract price** of General Conditions of Contract.

Bank Guarantee in the form given in Section -2 in favor of Chief General Manager/IT, of Customer (TSSPDCL), which should be valid up to a period till 28 days beyond completion of intended date of completion of contract (4 months)+28 days.

(Or)

Bank Draft, in favor of Pay Officer, TSSPDCL, payable at Customer Headquarters (Hyderabad) drawn on any Nationalized / Scheduled Bank.

31.2 If the Performance Security is provided by the successful Bidder in the form of a Bank Guarantee, it shall be issued by Nationalized / Scheduled Indian Bank and acceptable to the Employer.

31.3 Failure of the successful Bidder to comply with the requirements under this Section shall constitute sufficient grounds sufficient grounds for cancellation of the award and forfeiture of the Bid Security.

32. CORRUPT OR FRAUDULENT PRACTICES

32.1 Employer expects that Bidders / Bidders / Contractors observe the highest standard of ethics during the procurement and execution of such contracts. In Pursuance of this policy, the Employer:

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

(i) "**Corrupt practice**" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution, and

(ii) "**Fraudulent Practice**" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Employer, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Employer of the benefits of free and open competition.

(iii) Will reject a proposal for award if it is determined that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

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

32.2 Furthermore, Bidders shall be aware of the provision stated in above Clauses and Sub-Clause of the General Conditions of Contract.

33. Monitoring of Contract

a. The bidder shall ensure that the required Man power as per the contract is deployed.
b. If delay in providing the desired quality of people is observed a performance notice would be given to the selected bidder to speed up the deployment process.

c. Any Change in the constitution of the firm, etc. Shall be notified forth with by the Contract or in writing to the tendering authority and such change shall not relieve any former member of the firm, etc., from any liability under the contract.
d. No new business partner/partners shall be accepted in the firm by the selected bidder in Respect of the contract unless he/they agree to abide by all its terms, conditions and Deposits with the tendering authority through a written agreement to this effect. The bidder's receipt for acknowledge mentor that of any partners subsequently accepted as above shall be in the all of them and will be sufficient discharge of or any of the purpose of the contract.
e. The selected vendor shall not assign or let this contract or any substantial part thereof to any other agency without the permission of tendering authority except the one with whom the Bidder has collaborated or the purpose of execution of the project.

34. Right to Vary Number of Resources

a. At the time the Contract is awarded, the number of people originally specified in the bidding document may be increased or decreased, provided this change does not exceed the limits/ceilings of minimum and maximum quantity as specified in S.No. II below.
b. Unless otherwise specified in the bidding document, if the order is placed up to25%in excess of the number of people required, the bidder shall be bound to meet the required number without any change in the rates quoted or other terms and conditions of the bid and the bidding document.
c. Enhancement of the agreement value also may be made by TSSPDCL with the rates and conditions given in the entered agreement depending services required has to be enhanced as per the requirement of the utility. The terms & conditions applicable on the new people thus engaged will remain the same as those for the people engaged earlier.
d. If the tendering authority does not engage of the selected person/s or engages less number of people than the quantity indicated in the tender, the bidder shall not be entitled to claim any compensation and corresponding rate of designated service category/ person shall not be payable.

35. Responsibilities of the Man Power of selected bidder

a. The deployed manpower of the Bidder will maintain office decorum. They will be courteous, polite and cooperative.
b. The deployed manpower will adhere to the office timings of the Employer and follow all rules, regulations and policies as decided by the Customers.
c. The deployed manpower Bidder will be responsible for any damage to equipments, property and third party liabilities caused by their act since the premise of the Customers. They will us all equipment only for the purpose of carrying out their legitimate business of the Customers and will not put to any other use. For any damages, the extent of damage as decided by the Customers will be final.
d. The vendor will need to possess multi-dimensional capability to adequately meet the requirement of the contract/ award;
e. The vendor & its designated man power will need to be able to work efficiently with senior management and officers of Customers;
f. The vendor will bring proven knowledge and experience of handling project monitoring and efficiency improvement assignments.
g. Thevendoranditsdesignatedmanpowershallbringtheirownlaptopsanddatacardfor carrying out their activities.

36. Recoveries from vendor

a. Recovery of liquidated damages and penalties shall be made from bills and/or the first available opportunity.
b. The Employer shall withhold amount to the extent of non-deployment of resources or non-performance of services until all the contractual service agreements are met satisfactorily. In case of failure to withhold the amount, it shall be recovered from his dues and performance security deposit available with the Company.
c. The balance, if any, shall be demanded from the Bidder and when recovery is not possible, the Employer shall take recourse to law in force.

SECTION-III

GENERAL TERMS & CONDITIONS

GENERAL

1. DEFINITIONS

Terms, which are defined in the Contract Data, are not defined in the Conditions of Contract but keep their defined meanings. Capital initials are used to identify defined terms.

Bill of Quantities means the prices and completed Bill of Quantities forming part of the Bid.

Completion Date means the date of completion of the Works as certified by the Engineer.

Contractor means the bidder or corporate body whose bid to carry out the works has been accepted by the employer.

Contract means the contract between the Employer and the Contractor, the terms and conditions of which have been incorporated in the agreement to be executed between the two parties, to execute, complete and maintain the Works.

Contract Data defines the documents and other information which comprise the bid accepted by the Employer.

Contractor's Bid means the completed Bidding document submitted by the Contractor to the Employer consisting of Technical bid and Price bid.

Contract Price means the price stated in the Letter of Acceptance and thereafter as adjusted in accordance with the provisions of the Contract.

Days are calendar days; **months** are calendar months.

Defect is any part of the works not completed in accordance with the contract.

Defects Liability Period is the period named in the Contract Data and calculated from the Completion Date.

Employer means the party who will employ the Contractor to carry out the works.

Engineer means the person named in the Contract Data (or any other competent person appointed and notified to the contractor to act in replacement of the Engineer) who is responsible for supervising the Contract, administering the Contract, certifying payments due to the Contractor, issuing and valuing Variations to the Contract, awarding extensions of time, and valuing the Compensation Events.

Equipment means the Contractor's machinery and vehicles brought temporarily to the Site to construct the Works.

Initial Contact Price means the Contract Price listed in the Employer's Letter of Acceptance.

Intended Completion Date means the date on which it is intended that the Contractor shall complete the Works. The Intended Completion Date is specified in the Contract Data. The Intended Completion Date may be revised only by the Employer by issuing an extension of time.

Materials are all supplies, including consumables, used by the Contractor for incorporation in the Works.

Plant is any integral part of the Works which is to have a mechanical, electrical, electronic or chemical or biological function.

Site is the area defined as such in the Contract Data.

Site Investigation Reports are those which were included in the Bidding documents and are factual interpretative reports about the surface and sub-surface conditions at the site.

Specification means the Specification of the Works included in the Contract and any modification or addition made or approved by the Engineer.

Start Date is given in the Contract Data and is the date of receipt of the Letter of Acceptance by the contractor.

Subcontractor means a person or corporate body who has a Contract with the Contractor to carry out a part of the work in the Contract which includes work on the Site.

Temporary Works are works designed, constructed, installed, and removed by the Contractor, which are needed for construction or installation of the Works.

Variation is an instruction given by the Engineer, which varies the Works.

The Works are what the Contract requires the Contractor to construct, install and turn over to the Employer, as defined in the Contract Data.

2 Extension in Delivery Period and Liquidated Damages (LD)

a) Except as provided under clause "Force Majeure", if the Bidder fails to deploy the requisite manpower and providing of requisite services within the period specified in the Contract, the Employer may without prejudice to all its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to the percentage specified in the conditions of the Contract Price for each week or part thereof of delay until actual deployment of the manpower and providing of requisite services, up to a maximum deduction of the percentage specified in the bidding document and/ or contract. Once the maximum is reached, the Employer may terminate the Contract pursuant to clause "Termination".

b) The time specified for services in the RFP bid document shall be deemed to be the essence of the contract and the successful Bidder shall arrange manpower for deployment within the specified period.

c) The service provider shall request in writing giving reasons for extending the deployment period of manpower and providing requisite services if he finds himself unable to arrange requirement of award within the stipulated delivery period. This request shall be submitted as soon as a hindrance occurs or within 15 days from such occurrence but before expiry of stipulated period of completion of deployment schedule after which such request shall not be entertained.

d) The justification of causes of hindrance in the execution of award will be examined and the period of delay occurred due to that and recommends the competent authority on the period of extension which would be granted with or without liquidated damages.

e) Normally, extension in deployment of manpower in following circumstances may be considered without liquidated damages:
• When delay has occurred due to occurrence of some unfortunate event to any of the selected manpower
• When delay has occurred due to resignation of the selected manpower or accident or demise etc.

f) It shall be at the discretion of the concerned authority to accept or not to accept the selected bidder after the expiry of the stipulated deployment period, if no formal extension in completion period has been applied and granted. The competent authority shall have right to cancel the contract with on the basis of contractual obligations not met.

g) For any delay in project implementation, the liquidated damages shall be imposed at the rate of 0.5% per week, subject to a maximum of 5% of the total value of the contract.

3. Limitation of Liability

Except in cases of gross negligence or willful misconduct: -

a) neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Bidder to pay liquidated damages to the Employer; and

b) The aggregate liability of the Bidder to the Employer, whether under the Contract, in tort, or otherwise, shall not exceed the amount specified in the Contract, provided

that this limitation shall not apply to any obligation of the Bidder to indemnify the Employer with respect to patent infringement.

4. Change in Laws & Regulations

Unless otherwise specified in the Contract, if after the date of the Invitation for Bids, any law, regulation, ordinance, order or bylaw having the force of law is enacted, promulgated, abrogated, or changed in Telangana / India, where the Site is located (which shall be deemed to include any change in interpretation or application by the competent authorities) that subsequently affects the Deployment Date and/ or the Contract Price, then such Deployment Date and/ or Contract Price shall be correspondingly increased or decreased, to the extent that the BIDDER has thereby been affected in the performance of any of its obligations under the Contract. Notwithstanding the foregoing, such additional or reduced cost shall not be separately paid or credited if the same has already been accounted for in the price adjustment provisions where applicable, in accordance with clause "Contract Price".

5. Force Majeure

a) The vendor shall not be liable for forfeiture of its Performance Security deposit, liquidated damages, or termination for default if and to the extent that it is delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

b) For purposes of this clause, "Force Majeure" means an event or situation beyond the control of the Bidder that is not foreseeable, is unavoidable, and its origin is not due to negligence or lack of care on the part of the vendor. Such events may include, but not be limited to, acts of the Employer in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.

c) If a Force Majeure situation arises, the contractor shall promptly notify the department in writing of such conditions and cause thereof within 15 days of occurrence of such event. Unless otherwise directed by Customer the contractor shall continue to perform its obligations under the contract as far as reasonably practical.

d) If the performance in whole or part or any obligation under the contract is prevented or delayed by any reason of Force Majeure for a period exceeding 60 days, either party at its option may terminate the contract without any financial repercussion on either side.

e) In case a Force Majeure situation occurs with the Customer, the Customer may take the case with the contractor on similar lines.

6. Change Orders and Contract Amendments

a) The Employer may at anytime order the Bidder/ selected vendor through Notice in accordance with clause "Notices" above, to make changes within the general scope of the Contract if this becomes necessary.

b) If any such change causes an increase or decrease in the cost of, or the time required for, the selected bidder's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or in the Delivery of Bidder and the Contract shall accordingly be amended. Any claims by the selected vendor for adjustment under this clause must be asserted within thirty (30) days from the date of the selected BIDDER receipt of the Employer's change order.

c) Prices to be charged by the selected vendor for any related services that might be needed but which were not included in the Contract shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the selected BIDDER for similar services.

7. TERMINATION

7.1 Termination for Default

i. The tender sanctioning authority of the Customer may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the contractor, terminate the contract in whole or in part: -

a. If the contractor has provided or replaced resources inferior to that which were selected at the time of bidding even after being provided sufficient time to fulfill its obligations.

b. If the contractor fails to perform any other obligation under the contract within the specified period of delivery of service or any extension granted thereof; or

c. If the contractor, in the judgment of the Employer has engaged in corrupt, fraudulent, collusive, or coercive practices in competing for or in executing the contract.

d. If the contractor commits breach of any condition of the contract.

ii. If the respective Customer, terminates the contract in whole or in part then amount of performance security deposit (PSD) and due payments, if any, will be forfeited.

iii. Before cancelling a contract and taking further action ,advice of senior most finance person available in the office and of legal adviser or legal assistant posted in the office, if there is one, may be obtained.

7.2 Termination for Insolvency

The respective Customer may at any time terminate the Contract by giving Notice to the BIDDER if the BIDDER becomes bankrupt or otherwise insolvent. In such event, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to Customer.

7.3 Termination for Convenience

i. T h e Customer may, by Notice sent to the BIDDER, may terminate the Contract, in whole or in part, at any time for its convenience. The Notice of termination shall specify that termination is for the Employer's convenience, the extent to which performance of the Bidder under the Contract is terminated ,and the date upon which such termination becomes effective.

ii. Depending on merits of the case the BIDDER may be appropriately compensated on mutually agreed terms for the loss incurred by the contract if any due to such termination.

8. Settlement of Disputes

8.1 If any dispute or difference of any kind whatsoever will arise between the Employer and the Bidder in connection with or arising out of the Contract, the parties will make every effort to resolve amicably such dispute or difference by mutual consultation.

8.2 If, after thirty (30) days the parties have failed to resolve their dispute or difference by such mutual consultation, then either the Employer or the Bidder may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

8.3 Any dispute of difference in respect of which a notice of intention to commence arbitration has been given in accordance with this Clause will be finally settled by arbitration. Arbitration may be commenced prior to or after delivery of the Materials /equipment under the Contract.

8.4 Arbitration proceedings will be conducted in accordance with the following rules of procedure**.** The dispute resolution mechanism will be as follows:

a. In the case of a dispute or difference arising between the Employer and a Bidder relating to any matter arising out of or connected with this agreement, such dispute or difference will be settled in accordance with the Arbitration and

Conciliation Act. 1996. The Arbitral Tribunal will consist of three Arbitrators one each to be appointed by the Employer and the Bidder the Third Arbitrator will be chosen by the two Arbitrators so appointed by the parties and will acts as Presiding Arbitrator. In case of failure of the two Arbitrators appointed by the parties to reach upon a consensus within period of 30 days from the appointment of the Arbitrator appointed subsequently, the Presiding Arbitrator will be appointed by The Institution of Engineers (India).

b. If one of the Parties fails to appoint its Arbitrator in pursuance of Sub-Clause (a) within 30 days after receipt of the notice of the appointment of its Arbitrator by The Institution of Engineers (India), will appoint the Arbitrator. A certified copy of the order of the Institution of Engineers (India), making such an appointment will be furnished to each to the parties.

c. Arbitration Proceedings will be held at Employer's Headquarters, and the language of the Arbitration Proceedings and that of all documents and communication between the parties will be English.

d. The decision of the majority of Arbitrators will be final and binding upon both parties. The cost and expenses of Arbitration Proceedings will be paid as determined by the Arbitral Tribunal. However, the expenses incurred by each party in connection with the preparation, presentation etc., of its proceedings as also the fees and expenses paid to the Arbitrator appointed by such party or on its behalf will be borne by each party itself.

e. Where the value of the Contract is Rs. One Crore and below, the disputes or differences arising will be referred to the Sole Arbitrator. The Sole Arbitrator should be appointed by agreement between the parties; failing such agreement, by the appointing authority namely The Institution of Engineers (India).

8.5 **Notwithstanding any reference to arbitration herein,**

The parties will continue to perform their respective obligations under the Contract unless they otherwise agree; and

The Employer will pay the Bidder any monies due the Bidder.

9. Jurisdiction

All and any disputes or differences arising out of or touching this contract will be decided by the Courts or Tribunals situated in Employer's Headquarters only. No suit or other legal proceedings will be instituted elsewhere.

10. Notices

10.1 Any notice given by one party to the other pursuant to this Contract will be sent to the other party in writing or by cable, telex, or facsimile and confirmed in writing to the other party's address.

10.2 A notice will be effective when delivered or on the notice's effective date, whichever is later.

SECTION-IV
QUALIFICATION REQUIREMENTS

1. The Bidder should be a company/firm registered in India with at least five (5) years experience of providing IT Security Audit. Documentary evidence should be produced in support of experience
2. The Bidder must have done at least three Security Audit assignments (Application Security Audit and VAPT) of which at least one should be Application Security Audit in last three years. Documentary evidence should be produced in support of audit assignments.
3. The Bidder should be CERT-In (Computer Emergency Response Team - India) empanelled Agency (Year-2021) with at least three professionals. Out of three professionals, any of two should have CISA/CISM/CISSP/CEH certifications. Bidder should produce documentary evidence of the certifications.
4. The Bidder or Consortium Partner should not be blacklisted by any institution in India or abroad. (Self-declaration to be provided).
5. The bidder must be a profit making firm, during the last 3 years, with annual turnover of not less than Rs.3 Crores, in each of past three financial years (2017-18, 2018-19, 2019-20) with a positive net worth. Financial Turnover certified by CA, as per latest RBI guidelines, is to be submitted.

SECTION-V

SCOPE OF WORK

The implementation of Cyber security measures in TSSPDCL, aims at implementing ISMS, ISO 27001 Certification for TSSPDCL Data Center & SCADA Center, identifying the gaps & arresting all possible vulnerabilities existing in the IT Network/Hardware & IT Applications of the Data Center & SCADA Center of TSSPDCL. The scope of work includes the following;

1 Preparation of all the policy documents needed for ISMS and implementing the same. ISO 27001:2013(or latest) certification has to be provided in conformity with ISO/IEC 27019, in accordance with Annexure-XI for TSSPDCL Data Centre and SCADA Centre at Hyderabad and its related equipment. Review & Update/Maintain the ISMS documents in case of any changes, for a period of 3 years.

2 Preparation of Cyber Crisis Management Plan in accordance with Annexure-XI.

3 The vendor shall document the Cyber Security Policy, a Cyber Risk Assessment and Mitigation Plan. The Cyber Risk Assessment and Mitigation Plan shall be drawn upon the best practices being followed globally in the Power Sector. It shall contain a clearly defined risk assessment matrix for both IT and OT environment and the latest modified risk acceptance criteria adopted by the Discom.

4 Mock drill exercises shall be conducted for identifying the shortcoming(s), if any, and to improve preparedness to handle cyber breach/incidents, in accordance with Annexure-XI .

5 Perform VAPT (Vulnerability Assessment and Penetration Testing) of IT Systems and Security Audit of TSSPDCL's online applications including its websites, from internal and external perspective. The results should clearly articulate security issues and recommendations.

6 The Cyber Security Audit (VAPT, Application Security etc.,) shall be as per ISO / IEC 27001:2013(or latest) along with sector specific standard ISO/IEC 27019, IS 16335 and other applicable guidelines in accordance with Annexure-XI .

7 A Comprehensive Cyber Security Audit including VAPT, has to be carried out every 6 months to keep the IT system, Security Compliant, for a period of 3 years, from the date of award of work.

8 Detailed Study of the existing IT Infrastructure at TSSPDCL Data Center and SCADA Center, has to be done and identify the probable threats facing organization's information assets. A detailed report along with recommendations on the Security infrastructure to be provided, is to be submitted. Based on the recommendations, the required Security infrastructure will be procured by the Discom, for safeguarding the IT infrastructure.

9 Necessary assistance & guidance to be provided by the Auditor for closure of the gaps and identified vulnerabilities in all the audited IT Systems. After closure of all the gaps, vulnerability checks have to be re-conducted to ascertain the closure of all the vulnerabilities in the TSSPDCL IT Systems and final Individual Audit Compliance Certificates to be submitted for all the audited IT Applications and Systems

10 The List of Software Applications proposed for Security Audit to examine the security risks (like Data Security, SQL Injection, XSS Scripting, DOS attacks, Access rights & violations,

Back-end modification etc.,) along with risk report, suggestive actions and certifications, are as below;

Sl. No	IT Applications
1.	**Online Applications :** Website , CSC, HT Billing, EBS, CCC, HTCSC, SAS, Legal, MATS, Medical, OMS, SCADA, etc.
2.	**Mobile Application**: TSSPDCL Mobile App in Android & iOS.

11 The list of existing Assets proposed for VAPT are as below;

IT Hardware			
Sl. No.	**Asset Type**	**No. of items**	**Location**
1	Servers-Windows (Physical or Virtual)	10	Data Center and SCADA Center, Hyderabad
2	Servers-Linux (Virtual/ Physical)	23	
3	Servers-Desktops and Other Devices	10	
4	Database-Backup Management	2	
5	Database-RAC	3	
Network Devices			
8	Network-Firewall	3	Data Center and SCADA Center, Hyderabad
9	Network-IPs (Public)	15	
10	Network-Load Balancer	2	
11	Network-Routers	5	
12	Wi-Fi Router	1	
13	Network-Switches	14	
14	Proxy Server	1	

Note:. The list mentioned above are only indicative figures. Actuals may vary.

12 The VAPT assessment shall involve the following -

5.1 Vulnerability Assessment:

a. Identification of potential vulnerabilities & suggest remedies.
b. Identification of ports and services running on them & provide suitable solutions.
c. Systems and OS fingerprinting.
d. Application version specific vulnerabilities and suggest best practices.
e. Review of Business process
f. Resource utilization of servers & applications

5.2 Penetration Testing:

a. Exploiting identified vulnerabilities ensuring that no loss of data occurs due to such penetration testing.
b. Password strength service testing.
c. Mitigation plan for patching the exploited vulnerabilities.

5.3 Server Assessment

a. Data security for each server/equipment.
b. Logical access controls for each Server/equipment.
c. Operating system review including vulnerability Assessment for each equipment.

5.4 Network Architecture:

a. Review of TSSPDCL Network Architecture along with Modification Recommendations based on Standard practices.
b. Review & suggest a topography of the network architecture to avoid attacks of external/internal intruders on network.
c. Review & suggest the network segregation into various trusted/untrusted /DMZ zones
d. Review of entry and exit points of the TSSPDCL network along with the security measures implemented on the same.

etc.

13 **Non-Disclosure Clause:** The selected bidder will have to maintain secrecy of the knowledge & procedure acquired through the audit process of TSSPDCL.

14 **Deliverables:**

a. Executive summary and detailed audit report on the core findings and Risk Analysis of the IT System of TSSPDCL
b. Detailed Analysis report on security assessment along with corrective measures and suggestions.
c. Detailed Vulnerability assessment report with risk categorization (High, Medium, Low) and the step by step remediation plan to patch the identified vulnerabilities.
d. Penetration Testing Report with exploited vulnerabilities and PoC along with the remedies.
e. Configuration review report of network devices and recommendations to patch the identified vulnerabilities is to be submitted
f. A detailed report along with recommendations on the Security infrastructure and license subscriptions needed for a secured IT setup, as per the latest technology, is to be submitted.
g. Individual Security Audit Compliance Certificates to be provided for all the audited IT Applications and Systems, after closure of all the gaps and vulnerabilities in the TSSPDCL IT Systems. These certificates have to be renewed on every expiry, till 3 years.
h. ISMS Documentation in full shape.
i. ISO 27001 certification for a period of 3 years.
j. Training to be imparted to the concerned Discom Officers on IT security awareness and maintenance of Security measures and training records.

SECTION-VI

PAYMENT & PENALTY

6.1 Fees and Payment Terms

1. The Payment shall be made against achievement of milestones as per the following payment schedule;

S.No.	Phase	Amount to be paid (in % of Contract value)
1.	Completion of VAPT & Security Audit of all IT Applications as per the scope given, submission of initial report and ISMS Documentation in full shape.	30%
2.	ISO27001 Certification and Submission of Final Closure report for all gaps and submission of all relevant Security Audit certificates.	40%
3.	Subsequent Half-yearly Application Security Audit , VAPT and Renewal of any expired certifications;	
	i) at the end of 1st 6 months period	5%
	ii) at the end of 2nd 6 months period	5%
	iii) at the end of 3rd 6 months period	5%
	iv) at the end of 4th 6 months period	5%
	v) at the end of final 6 months period	10%

2. The vendor shall raise invoices for services rendered in triplicate as per payment schedule to the respective controlling officers, who will forward the bills to the paying authority through the Chief General Manager/IT after due authentication and certification, for effective payment. The payment for above work will be made by Pay Officer, of respective Customers after verification of the bills by the CGM(IT) designated for the purpose.
3. Necessary statutory deductions, as applicable, are to be made against each phase of payment. However, any delay in payment will not entitle the contractor for any compensation or form ground for extension in delivery period without liquidated damages.
4. The currency or currencies in which payments shall be made to the vendor under this Contract shall be Indian Rupees (INR) only.
5. All remittance charges will be borne by the selected bidder.
6. In case of disputes, 20% of the amount shall be withheld and will be paid only after settlement of the dispute.
7. Payment schedule for the bid will be on Pro rata basis after the computation and deduction of all applicable penalties.
8. If any mentioned work is not required to be executed, due to any reason whatsoever: the proportionate cost of the contract fee may be deducted on pro-rata basis, as may be mutually agreed between the Employer and bidder.
9. Extension of period of assignment: Extension of time schedule as referred in Scope of Works, above may be considered. In case the project work is extended beyond the contract period in the event of delay(s) not attributable to the Bidder, respective Customer may consider for payment of contract fee on mutually agreed terms.

6.2 Penalty Clause

1. Penalty for delay in project implementation:

   For any delay in project implementation, the liquidated damages shall be imposed at the rate of 0.5% per week, subject to a maximum of 5% of the total value of the contract.

2. Penalty would be deducted from the applicable payments. All applicable penalties will be in addition to liquidated damages.

6.3 TERMINATION CLAUSE.

The Customer reserves the right to terminate this contract at any point of time without assigning any reasons thereof.

Section-VII

FORMS & ANNEXURES

TECHNICAL PROPOSAL–STANDARD FORMS

Annexure I: Technical Bid Proposal Format:

Annexure I-A: Technical Proposal submission forms

Annexure I-B: Firm's references.

Annexure I-C: Team composition and task assignments.

Annexure I-D: Format of Curriculum Vitae of proposed key professional staff.

Annexure II: Eligibility Criteria references

Annexure III: Bidders Authorization Certificate

Annexure IV: Self-Declaration- No Blacklisting

AnnexureV: Financial Proposal- Standard Forms

AnnexureV-A: Financial Proposal Submission Letter

AnnexureV-B: Financial Bid Format

AnnexureVI: Pre-Bid Queries Format

AnnexureVII: Draft Agreement Format

AnnexureVIII: Bid Security Form

Annexure IX: Performance Security Bank Guarantee

AnnexureX: Details to be furnished by the Bidder

Annexure I:

Technical Bid Proposal Format:

S.No	Item Description	UoM	Qty	Compliance Yes/No
1	Security Audit of IT Applications in TSSPDCL viz. Website , CSC, HT Billing, EBS, CCC, HTCSC, SAS, Legal, MATS, Medical, OMS, SCADA along with report generation and certification.	LS	1	
2	Security Audit of TSSPDCL Mobile Apps in Android & iOS, along with report generation and certification.	LS	1	
3.	VAPT of IT Critical Infrastructure as listed in the Scope of work(Section-V) along with necessary reports and solution document	LS	1	
4.	Implementation & Documentation for ISMS including preparation of CCMP and ISO27001 certification for TSSPDCL Data Centre and SCADA Centre, with a validity period of 3 years.	LS	1	
5.	Half-Yearly Security Audit of IT Applications, Mobile Apps (Android & iOS) and VAPT of Critical IT Infrastructure, for Gap Analysis and Closure of Gaps, for a period of 3 years, with renewed certification, for keeping the System Security compliant.	LS	1	

Annexure I-A:

TECHNICAL PROPOSAL SUBMISSION FORM

(on company's letterhead) [Location, Date]
FROM: (Name of Firm)
_____

To:
Chief General Manager/IT,
1st Floor, Corporate Office,
Mint Compound,
HYDERABAD

Reference: NIT No. _____: Dated: _____

Subject: Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad.

Dear Sir/ Madam,

We, the undersigned, offer to provide the services for the above in accordance with your Request for Proposal dated [Date], and our Proposal. We are hereby submitting our Proposal, which includes this Technical Proposal, and a Financial Proposal sealed under a separate envelope.

If negotiations are held during the period of validity of the Proposal, i.e., before [Date] we undertake to negotiate on the basis of the proposed services. Our Proposal is binding upon us and subject to the modifications resulting from contract negotiations.

We understand you are not bound to accept any Proposal you receive.

We remain,

Yours sincerely,

Authorized Signature:

Name and Title of Signatory:
Name of Firm:

Address:

AnnexureI-B:

FIRM'SREFERENCES

1. Bidders shall submit details of their experiences in following table in regard to scope of work and eligibility criteria of this RFP.

Sl. No.	**Name of utility where Assignment executed**	**Name of assignment**	**Scope of work of assignment in details**	**Location of assignments**	**Duration of the assignments**	**Value of Works executing/executed**
	1	2	3	4	5	6

PLACE:

SIGNATURE OF AUTHORISED SIGNATORY (BIDDER)

DATE:

COMPANY SEAL

NAME IN FULL
DESIGNATION /
STATUS IN THE FIRM
ADDRESS OF BIDDER

AnnexureI- C:

TEAM COMPOSITION AND TASK ASSIGNMENTS

List of Proposed Professionals:

Sl. No.	Name	Proposed role	Qualification	Experience	Reference page no of complete details in document
1.					
2.					
3.					
4.					
5.					

Signature:_____

(Authorized Representative)

Full Name: _____

Title: _____

Name of Firm _____

Address:_____

AnnexureI- D:

FORMAT OF CURRICULUM VITAE (CV) FOR PROPOSED KEY PROFESSIONAL STAFF

Proposed Position:

Name of Firm:

Name of Staff:

Profession:

Date of Birth:

Years with Firm/Entity:

Nationality:

Membership in Professional Societies:

Detailed Tasks Assigned:

Key Qualifications:

[Give an outline of staff member's experience and training most pertinent to tasks on assignment. Describe degree of responsibility held by staff member on relevant previous assignments and give dates and locations. Use about half a page.]

Education:

[Summarize college/university and other specialized education of staff member, giving names of schools, dates attended, and degrees obtained. Use about one quarter of a page.]

Employment Record:

[Starting with present position, list in reverse order every employment held. List all positions held by staff member since graduation, giving dates, names of employing organizations, titles of positions held, and locations of assignments. For experience in last ten years, also give types of activities performed and client references, where appropriate. Use about two pages.]

Languages:

[For each language indicate proficiency: excellent, good, fair, or poor; in speaking, reading, and writing]

Certification:

I, the undersigned, certify that to the best of my knowledge and belief, these data correctly describe me, my qualifications, and my experience.

_____Date: _____

[Signature of staff member and authorized representative of the Firm] Day/Month/Year

Full name of staff member:_____

Signature:_____
(Authorized Representative)
Full Name: _____
Title: _____
Name of Firm _____
Address**:** _____

Annexure II

ELIGIBILITY CRITERIA REFERENCES

(To be enclosed with the technical bid)

1. **Turnover of the Bidder**

Name of the Bidder	Turnover of the Bidder		
	2017-18	2018-19	2019-20

Certified Copies of audited Balance sheets with Profit &Loss account statement for last 3 years must be enclosed along with the bid.

PLACE:
SIGNATORY (BIDDER)
DATE:
COMPANY SEAL

SIGNATURE OF AUTHORISED

NAME IN FULL
DESIGNATION /
STATUS IN THE FIRM
ADDRESS OF BIDDER

Networth

Name of the Bidder	Networth of the Bidder		
	2017-18	2018-19	2019-20

Certified Copies of audited Balance sheets with Profit & Loss account statement for last 3 years must be enclosed along with the bid.

PLACE:
SIGNATORY (BIDDER)
DATE:
COMPANY SEAL

SIGNATURE OF AUTHORISED

NAME IN FULL
DESIGNATION /
STATUS IN THE FIRM
ADDRESS OF BIDDER

1. **Other Enclosures**

Sl. No	Qualification Requirements	Details of qualifying parameters	Reference (pageno)
1	The Bidder must be a company registered under the Companies Act, 1956 or a partnership firm Registered under Partnership Act or a Proprietorship	Self-attested copy of the Certificate of Incorporation, Registration Certificate and Certificate of Commencement of Business	
2	The bidder should be registered with the GST department	GST registration certificate Income Tax registration Certificate/Pan Card	
3	The Bidder would deposit Earnest money along with the Technical bid.	**Details** Banker's Cheque/DD No: Bank &Branch: Date: OR Bank guarantee No.: Date: Bank & branch	
4	The bidder must submit a letter of authorization from the Company authorizing a person to sign the documents on behalf of the company, submit technical, commercial information and attend meetings on behalf of the company.	Letter of authorization Company's letter head.	
5	The bidder must not have been blacklisted by the Central or any State Government or any of their institutions.	The bidder should provide an undertaking (self-certificate) that The bidder hasn't been blacklisted by the Government or any of their Institutions.	

Signature:_____
(Authorized Representative)
Full Name:_____
Title: _____
Name of Firm_____
Address:_____

Annexure III

BIDDER'S AUTHORIZATION CERTIFICATE
(To be enclosed with the technical bid)

To,
The CGM (IT.),
TSSPDCL,
Hyderabad

<Bidder's Employee Name> _____,<Designation> _____is hereby authorized to sign relevant documents on behalf of the company/ firm in dealing with Bid of reference <Bidder Name, Dept & Date> _____. He is also authorized to attend meetings & submit pre-qualification, technical & commercial information as may be required by you in the course of processing the above said Bid. For the purpose of validation, his/ her verified signatures are as under.

Thanking you,

Name of the Bidder: - Verified Signature:
Authorized Signatory: -
Seal of the Organization: -
Date:_____
Place:_____

Annexure IV

SELF-DECLARATION–NO BLACKLISTING

(To be enclosed with the technical bid)

To,
The CGM (IT)
TSSPDCL,
Hyderabad

In response to the Tender Ref No._____dated_____
Providing qualified and competent Bidders for "Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad**"** or a period of 4 months as an owner/ partner/ Director of_____, I/ We hereby declare that presently our Company/ firm_____is having unblemished record and is not declared ineligible for corrupt & fraudulent practices either indefinitely or for a particular period of time by any State/ Central Government/ PSU.

We further declare that presently our Company/ firm _____is not blacklisted and not declared ineligible for reasons other than corrupt & fraudulent practices by any State/ Central Government/ PSU on the date of Bid Submission.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

Thanking you,

Name of the Bidder: -
Authorised Signatory: -
Seal of the Organization: -
Date:
Place:

Annexure-V

FINANCIALPROPOSAL–STANDARDFORMS

Annexure V-A: Financial Proposal submission form.

Annexure V-B: Financial Bid Format

Annexure-V-A:

FINANCIAL PROPOSAL SUBMISSION LETTER

(on company's letterhead) [Location, Date]

FROM: (Name of Firm) TO:

_____

The CGM (IT)
TSSPDCL,
Hyderabad

Reference: NIT No. _____: Dated: _____

Subject: Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad.

Sir/ Madam:

We, the undersigned bidder, having read & examined in detail, the Bidding Document, the receipt of which is hereby duly acknowledged, I/ we, the undersigned, offer to supply/ work as mentioned in the Scope of the work in conformity with the said bidding document for the same.

I / We undertake that the prices are in conformity with the requirements. The quote/ price are exclusive of all costs likely to be incurred for executing this work. The prices are exclusive of all taxes which shall be paid extra, as per applicable law.

I/ We hereby declare that in case the contract is awarded to us, we shall submit the contract performance guarantee as prescribed in the bid document.

I / We agree to abide by this bid for a period of 90 days after the last date fixed for bid submission and it shall remain binding upon us and may be accepted at any time before the expiry of that period.

Until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and your notification of award shall constitute a binding Contract between us.

I/ We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We agree to all the terms & conditions as mentioned in the RFP bid document and submit that we have not submitted any deviations in this regard.

We understand you are not bound to accept any Proposal you receive.

We remain,

Yours sincerely,
Authorized Signature:
Name and Title of Signatory:
Name of Firm:
Address:

Annexure-V-B

FINANCIALBID FORMAT

RFP Bid Document No: CGM/IT/TSSPDCL/HYD/CYB-SECURITY/02/2021-22

Financial Offer for Appointment of Agency for "Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad". [To be submitted in duplicate]

To,
The Chief General Manager /IT,
TSSPDCL, Hyderabad.

SUB: " Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad**".**

Dear Sir,

We are submitting our financial offer in duplicate as follows:
Financial Proposal for "Implementation of Cyber Security measures for IT Systems at TSSPDCL Data Center and SCADA Center in Hyderabad".

Technical Bid Proposal Format:

S.No	Item Description	UoM	Qty	Unit Rate	Taxes and Duties on total qty.	Total in INR (Incl. taxes And duties)
1	Security Audit of IT Applications in TSSPDCL viz. Website , CSC, HTBilling, EBS, CCC, HTCSC, SAS, Legal, MATS, Medical, OMS, SCADA along with report generation and certification.	LS	1			
2	Security Audit of TSSPDCL Mobile Apps in Android & iOS, along with report generation and certification.	LS	1			
3.	VAPT of Critical IT Infrastructure as listed in the Scope of work(Section-V) along with necessary reports and solution document	LS	1			
4.	Implementation & Documentation for ISMS including preparation of CCMP and ISO27001 certification for TSSPDCL Data Centre and SCADA Centre, with a validity period of 3 years.	LS	1			
5.	Half-Yearly Security Audit of IT Applications, Mobile Apps(Android & iOS) and VAPT of Critical IT Infrastructure, for Gap Analysis and Closure of Gaps, for a period of 3 years, with renewed certification, for keeping the System Security compliant.	LS	1			

Note:

1. The above quantities are arrived based on the data existing, which may vary after surveying by the successful bidder once the order is placed.
2. The quantities mentioned in this financial bid are baseline quantities which are arrived only for evaluation of tender value.
3. The payments will be made as per the actual executed in field, either less or more.
4. The L1 Bidder will be evaluated based on the value arrived on the proposal given for existing and delta charges combined.

Name

Authorized signatory

Annexure-VI

PRE-BID QUERIES FORMAT

Name of the Company/Firm:

Tender Fee Receipt No._____Dated_____for Rs. _____

Name of Person(s) Representing the Company/Firm:

Name of Person	Company Name	Designation	Email-ID(s)	Tel.Nos.

Query/Clarification Sought:

S.No.	RFP Page No.	RFP Clause/Section No.	Clause Details	Query/Suggestion/ Clarification

Note: - Queries must be strictly submitted only in the prescribed format (DOC or PDF) through email or printed form at least **one day before the Pre-Bid Meeting**. Queries not submitted in the prescribed format and received after due date will not be considered/ responded at all by the tendering authority.

Annexure-VII
DRAFT AGREEMENT FORMAT

An agreement made this____(enter date of Agreement)between(enter your firm's name& address) (here in after called "the approved Bidder", which expression shall, where the context so admits, be deemed to include his heirs, successors, executors and administrators of the one part and the<TENDERINGAUTHORITY>which expression shall, where the contexts admits, be deemed to include his successors in office and assigns of the other part.

Whereas the successful bidder has agreed with the <tendering authority> to provide qualified and competent Bidder to the <tendering authority name and address>at its premises, all those articles set forth in our LOA._____Dated _____appended hereto in the manner set forth in the conditions of the bidding document and contract appended herewith and at the rates set forth in the said order(LOA).

And whereas the successful bidder has deposited a sum of Rs._____in the form of Bank Draft No./Banker Cheque/Bank Guarantee No._____dated._____ _____validup to_____.

Now these Presents witness:

1) In consideration of the payment to be made by the <tendering authority> through cheque/ DD at the rates set forth in the LOA hereto appended the successful bidder will duly provide the said Bidder as set forth in our LOA No. _____dated ___/ __ /20__thereof in the manner set forth in the NIT, Tender, Instructions to Bidders, Terms of Reference, General and Special Conditions of the Tender and Contract, Technical Bid and Financial Bid along with their enclosures.
2) The NIT, Tender, Instructions to Bidders, Terms of Reference, General and Special Conditions of the Tender and Contract, Technical Bid and Financial Bid along with their enclosures enclosed with the Tender Notice No._____dated.__/ __ /20__and also appended to this agreement will be deemed to be taken as part of this agreement and are binding on the parties executing this agreement.
3) Letter Nos. _____dated_____received from <bidder name> and letter Nos._____Dated _____issued by the <tendering authority> and appended to this agreement shall also form part of this agreement.
4) The <tendering authority> do hereby agree that if the successful bidder shall duly provide the said Bidder in the manner aforesaid to TSSPDCL in the said terms and conditions, the
<tendering authority> will through cheque/ DD pay or cause to be paid to the approved serviceprovider at the time and the manner set forth in the said conditions, the amount payable for each and every professional.
5) The deployment shall be affected and completed within the period as specified in the LOA.
6) In case of extension in the deployment period with liquidated damages, the recovery shall be made on the basis of percentages of value of the service category (as mentioned in the bidding document) which the bidder has failed deploy.

7) All disputes arising out of this agreement and all questions relating to the interpretation of this agreement shall be decided by the <tendering authority> and the decision of the <tendering authority> shall be final.
In witness where of the parties here to have set their hands on the _____day of__(Year) .

Signature of the Approved Bidder/bidder	Signature for and on behalf of <tendering authority>
Designation:	Designation:
Date:	Date:
Witness No.1	Witness No.1
Witness No.2	Witness No.2

Annexure-VIII

BID SECURITY FORM

Whereas. ..... (hereinafter called "the Bidder") has submitted its Bid dated (date of submission of bid) for the supply of. .....(name and /or description of the Materials / equipment) (hereinafter called "the Bid").

KNOW ALL PEOPLE by these presents that WE. .....(name of bank) having our registered office at. .....(address of bank)(hereinafter called "the Bank"), are bound unto. .....(name of Employer) (hereinafter called "the Employer") in the sum of for which payment well and truly to be made to the said Employer, 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
   a) withdraws its Bid during the period of bid validity specified by the Bidder on the Bid Form; or
   a) does not accept the correction of errors in accordance with the Bid Specification, or
2. If the Bidder, having been notified of the acceptance of its bid by the Employer during the period of bid validity;
   (a) fails or refuses to furnish the performance security, in accordance with the Bid Specification.
   (b) fails or refuses to execute the Contract Form if required; or

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

This guarantee will remain in force up to and including forty five (45) days after …….(Specification Date) the period of the bid validity, and any demand in respect thereof should reach the Bank not later than the above date.

. .....

(Signature of the Bank)

NOTE: This will be executed on a Rs.100/- non-judicial stamp paper issued by any **Nationalized/Scheduled** Bank.

Annexure IX

PERFORMANCE SECURITY BANK GUARANTEE

To,

_____,
_____,
_____,

1. Against contract vide advance acceptance of the Tender covering "Tender/ NIT Reference No._____dated _____and Project Titled"_____" (hereinafter called the said 'contract') entered into between {Department name} (hereinafter called the Employer) and _____ (hereinafter called the Bidder) this is to certify that at the request of the Bidder we _____Bank Ltd., are holding in trust in favour of the Employer, the amount of Rs_____(Rupees in words) to indemnify and keep indemnified the Employer against any loss or damage that may be caused to or suffered by the Employer by reason of any breach by the Bidder of any of the terms and conditions of the said contract and/ or in the performance thereof.

2. We agree that the decision of the Employer, whether breach of any of the terms and conditions of the said contract and/ or in the performance thereof has been committed by the Bidder and the amount of loss or damage that has been caused or suffered by the Employer shall be final and binding upon us and the amount of the said loss or damage shall be unconditionally paid by us forthwith on demand and without demur to the Employer.

3. We _____ Bank Ltd, further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for satisfactory performance and fulfillment in all respects of the said contract by the Bidder i.e. till_____hereinafter called the said date and that if any claim accrues or arises against us _____Bank Ltd, by virtue of this guarantee before the said date, the same shall be enforceable against us _____Bank Ltd, notwithstanding the fact that the same is enforced within ten months after the said date, provided that notice of any such claim has been given to us _____Bank Ltd, by the Employer before the said date. Payment under this letter of guarantee shall be made promptly upon our receipt of notice to that effect from the Employer.

4. It is fully understood that this guarantee is effective from the date of the said contract and that we_____Bank Ltd, undertake not to revoke this guarantee during its currency without the consent in writing of the Employer.

5. We undertake to pay to the Employer any money so demanded notwithstanding any dispute or disputes raised by the Bidder in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present bond being absolute and unequivocal.

6. The payment so made by us under this bond shall be a valid discharge of our liability for payment there under and the Bidder shall have no claim against us for making such payment.

7. We _____Bank Ltd, further agree that the Employer shall have the fullest liberty, without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by the Bidder from time to time or to postpone for any time or from time to time any of the powers exercisable by the Employer against the said Bidder and to forebear or enforce any of the terms and conditions relating to the said contract and we,_____Bank Ltd., shall not be released from our liability under this guarantee by reason of any such variation or extension being granted to the said Bidder or for any forbearance by the Employer to the said Bidder or for any forbearance and or omission on the part of the Employer or any other matter or thing whatsoever, which under the law relating to sureties, would, but for this provision have the effect of so releasing us from our liability under this guarantee.

8. This guarantee will not be discharged due to the change in the constitution of the Bank or the Bidder.

WITNESSNO.1

(Signature)
Full name and official
and Address (in legible letters)
with Bank stamp

WITNESS NO. 2

(Signature)

Full name and official

Address (in legible letters)

Authorised Bank Representative

(Signature)
Full name, designation
Address (in legible letters)

Attorney as per power of

Attorney No.....

Dated…….

Annexure-X

DETAILS TO BE FURNISHED BY THE Bidder

1. RFP No.	:	
2. Last date and time for submission of Bid	:	
3. Date and time for opening of Bid	:	
4. State whether Bid security is enclosed	:	
5. State whether the quotation in two parts has been submitted.	:	
6. Whether willing to furnish performance B.G**.** @ 5% if order is placed	:	
7. Prices whether Firm	:	
8.Financial Turnover certified by CA as per RBI guidelines, as mentioned in Eligibility criteria.		
9. Whether any other tax / duty payable. If so give details and the same is included / not included.	:	
10. State whether TSSPDCL terms of payment are accepted.	:	
11. State whether 120 days validity offered	:	
12. Whether Bid security exemption letter enclosed, if exempted in case of Govt. firms.	:	
13.Firm's references to showcase relevant experience along with necessary proofs and credentials		
14.Details of key personnel proposed to be engaged in the project		
15. Whether Income-tax clearance certificate enclosed.	:	
16. Whether Penalty clause accepted	:	

Place :

Date :

Signature of the Bidder :

Name :

Business address :

Annexure-XI

CEA (Cyber Security in Power Sector) Regulation, 2021

Cyber Security Controls and Measures

Regulation 3 Cyber Security Controls.

R.1 The Responsible Entity shall be mandatorily ISO/IEC 27001 certified (including sector specific controls like ISO/IEC 27019 for power sector).

R.2 The Responsible Entity shall have a documented Cyber Security Policy, drawn upon the guidelines issued by NCIIPC. The Cyber Security Policy shall amplify and resonate with the commitment and ability of the Responsible Entity, to secure its Critical Information Infrastructure(s) and also the Protected System(s). The Cyber Security Policy shall leverage state-of-art cyber security technologies to mitigate the cyber security risks, like multiple layered Access Management Process.

R.3 The Responsible Entity shall make readily available, the most recently updated Cyber Security Policy document to all Employees, who have access to, or are responsible for operating and securing Critical Information Infrastructure(s) and the Protected System(s) owned and/or operated by the Responsible Entity.

R.4 The Responsible Entity shall ensure annually review of the Cyber Security Policy by ISD. Any change(s) to be made in the Cyber Security Policy for strengthening the cyber security posture and improving cyber resilience framework, shall be made only with the due approval of Board of Directors.

R.5 The CISO shall be responsible and accountable to implement the Cyber Security Policy faithfully, through the Information Security Division.

R.6 ISD shall on a quarterly basis review the implementation of the cyber security policy and such review must include:

1) review of current cyber security and resilience capabilities of cyber Systems.
2) goals for a target level of cyber resilience and
3) plan(s) to improve and strengthen cyber security and cyber resilience 4) measures for improvement in Cyber Security posture.

R.7 The CISO shall record the reason(s) for exemption required, if any, in case, unable to comply with any of the provision(s) of the Cyber Security Policy. Any exception shall be allowed only when the compensatory control(s) to mitigate residual cyber security risks have been duly provisioned and the due approval as laid in the Change Management Process has been accorded by the Responsible Entity.

R.8 The CISO shall record the exemptions sought in statement of applicability controls, while getting the ISO 27001 certified. All needed exemptions and its justification shall be in synchronisation with Cyber Security Policy.

R.9 The CISO shall be responsible and accountable for ensuring implementation of CCMP by the ISD, during a cyber-crisis, as and when cyber crisis is declared by the designated Officer. (refer Regulation 29, R.4).

R.10 The CISO shall be responsible for implementation and regular review of the Cyber Risk Assessment and Mitigation Plan, on the basis of internal and external feedbacks and cyber threat intelligence gathered by ISD.

Regulation 4 Cyber Security Measures

R.1 The Responsible Entity shall ensure that its Employees and Employees of contractors and service vendors, having authorized cyber or physical (escorted or unescorted) access to Critical Cyber Assets, have undergone an adequate level of personnel risk assessment, cyber security awareness and training.

R.2 The Responsible Entity shall ensure that its Cyber Assets are not discoverable by any external Entity, unless permissible under the provisions of Cyber Security Policy or explicit policy decision has been taken otherwise.

R.3 The Responsible Entity shall formulate an Internet access policy, to monitor and regulate the use of the Internet, Internet-based services and Internet

connected devices by its Employees, e.g. social media sites, cloud-based internet storage sites, etc.

R.4 The Responsible Entity shall develop procedures for monitoring access by user that shall:

1) monitor for failed login attempts and account lockouts,
2) ensure proper handling of requests for username and password changes as well as procedures for authenticating anomalous or unusual customer requests,
3) regularly review System for any changes required in hardware and software,
4) ensure that any changes if required are approved and properly implemented and has provision for investigation if any anomaly is there.

R.5 The Responsible Entity before providing any remote access to its own Employee(s), or Employee(s)s of service and utility provider, shall evaluate the risk and potential impact in case of any compromise due to the Cyber Assets/resources being accessed remotely.

R.6 The Responsible Entity shall ensure that before grant of any remote access, Cyber Assets/resources are sufficiently hardened against external threats through the use of firewalls and other appropriate access control mechanisms. Further the access to these Assets/resources shall be limited to bare minimum that is deemed essential.

R.7 The Responsible Entity for processing request for remote access shall implement and test, a prototype of the design and shall evaluate the test results. The prototype of the design may be tested and evaluated for:

1) connectivity,
2) traffic protection,
3) authentication,
4) management, 5) logging,
6) performance,
7) implementation security, and
8) interference with other applications.

R.8 The Responsible Entity shall ensure that the security controls to be defined in the Cyber Security Policy pertaining to authorised or unauthorized remote access, shall be based on the following inherent assumptions:

1) that the command and control of Cyber Assets/resources if gained by malicious entities, shall attempt to extract sensitive data from the devices or through leveraged privileges to devices access try to gain access to IT and in particular, OT systems of the Responsible Entity with objective to cause service/system disruption and damage.
2) that the networks for remote access cannot be trusted, hence further network segmentation/security is must.
3) that remote end devices are highly infected with malware.

R.9 The Responsible Entity operating Substations remotely shall ensure that all such Substations are protected with multi layered ruggedized firewalls along with

Intrusion Prevention Systems (IPS). e.g. verification of source addresses (IP addresses) not only at the substation's external interface (Firewall), but also by the target component.

Sectoral CERTs may add requirement on

Independent, fault tolerant implantation of critical plant/SCADA safety functions.

ISO/IEC 27002:2013/27019:2017 9.4.1, 13.1.3, 14.2.4, 14.2.7, 17.2.1

R.10 The Responsible Entity shall install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect its IT, OT and ICS infrastructure from security exposures originating from internal and external sources. Segregation of IT network, OT network and ICS network, through DMZ (Demilitarized Zone) and separation via firewalls and authentication checks must be implemented.

R.11 The Responsible Entity shall install Anti-virus software on all servers and other computer systems. Regular updating of Anti-virus definition files and

automatic anti-virus scanning shall be ensured by the Responsible Entity. ICS devices which are resource constrained or for which anti-virus software is not available, shall have other ways of detecting intrusion, anomaly and changes in performance.

R.12 The Responsible Entity shall permit BYOD devices within its own network in rarest or rare instance, that to after establishing a separate, external, dedicated network for use of such BYOD. This network shall be secured and monitored in a manner consistent with those pertaining to remote access segments. The Responsible Entity may, if desired, use such a network for third-party-controlled client devices also.

R.13 The Responsible Entity shall determine and provide the resources needed for the establishment, implementation, maintenance and for continual improvement in the functioning of the ISD.

R.14 The Responsible Entity shall allocate sufficient Annual budget for enhancing cyber security posture, enhanced year over year and shall place the cyber security budget under disposal of CISO with checks and balance in place.

R.15 The Responsible Entity shall work in collaboration with other Industry Stakeholders as well as Academia to promote R&D activity in the domain of cyber security.

R.16 The Responsible Entity shall challenge their own cyber security ecosystems through the use of red /blue teams to introduce an adversary perspective in a controlled setting. Red teams serve to test for possible vulnerabilities and effectiveness of mitigating controls designed and implemented by the Responsible Entity. A red team may consist of own Employees of the Responsible Entity and/or outside experts, who are case independent of the security functions being tested.

Regulation 5 Access Control Policy

R.1 The Responsible Entity shall document and implement Access Control Policy to protect the Cyber Assets/Systems.

R.2 The Responsible Entity shall maintain a list of designated Employee(s) who are responsible for authorizing logical or physical access to protected Critical System or Critical Information. The Responsible Entity shall identify Employee(s) by Name, Designation, Official phone and the Critical System or Critical Information for which they have been designated for authorizing access.

R.2 The Responsible Entity shall ensure that provisions in the Access Control Policy for granting access to cyber assets/resources takes into account:

1) the observable state of the user (e.g. network account used and associated attributes)
2) the observable state of the requesting system (e.g. device characteristics like network location, installed credentials, etc) and
3) may include other behavioural attributes (automated user analytics, measured deviations from observed usage patterns)

R.3 The Responsible Entity shall ensure that the Access Control Policy must include the procedures and systems that shall:

1) limit access as appropriate, including during on boarding, transfers, and terminations
2) manage access permissions and authorizations, incorporating the principles of separation of duties and least privilege in order to restrict both visibility and accessibility.
3) re-certify user's access rights on a periodic basis (paying particular attention to accounts with elevated privileges including users, administrators, and service accounts)
4) addresses strong password controls for user's access to systems, applications, networks and databases. Password controls shall inter alia include: a) a change password upon first log on,

b) a change minimum password length and history,

c) password complexity as well as maximum validity period. 5) lock account access after 3 (three) failed log on attempts.
6) user credential data is stored using strong hashing algorithms.
7) utilize Multi-Factor Authentication (MFA) leveraging an application or Key fob or smart card to generate an additional verification code
8) deactivate access privileges immediately for Employee no longer employed by the Responsible Entity or whose access privileges have been withdrawn, including Employee of former service and utility providers.
9) not allow any Employee by virtue of rank or position, any intrinsic right to access confidential data, applications, system resources or facilities.
10) grant access requests, made from systems located on Responsible Entity owned network infrastructure, with the same security requirements as the access requests and communication from any other Entity owned network are granted. All communication shall be secured (encrypted and authenticated).
11) allow access to physical and logical assets and associated facilities, limited to authorized users, processes and devices. The access shall be managed consistently with the assessed risk of any unauthorized access percolating to authorized activities and transactions.
12) secure all components of telecommuting and remote access solutions, including client devices, remote access servers and internal servers accessed through remote access, against variety of threats.

R.4 The Access Control Policy shall ensure that access to individual cyber assets/resources is granted on a per-connection basis and only after successful trust evaluation of the entity requesting access. Further authentication for access to one resource shall not automatically mean grant of access to another resource(s) also.

R.5 The Responsible Entity shall ensure that the Access Control Policy is Cyber Asset/resource based and shall have the flexibility to vary on the sensitivity and criticality of the asset/resource/data.

R.6 The Responsible Entity shall ensure that the Access Control Policy inter alia has provision for checking that:
1) Users, devices, and other assets are authenticated commensurate with the risk of the access to the resource (e.g., individuals' security and privacy risks and other organizational risks)
2) Identities are proofed and bound to credentials and asserted in interactions
3) Physical access to assets is managed and protected.

R.7 The Access Control Policy shall provision using multiple remote access solutions depending on the needs of the remote access users, the criticality and associated risks of the Cyber Assets/resources/data to be accessed.

R.8 The Access Control Policy shall have provision for deploying additional controls and security measures to supervise Employee(s) with elevated system access entitlements (such as admin or privileged users). Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged user's activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

R.9 The Responsible Entity shall have requisite policies and procedures in place for the use of mobile devices like walkie-talkie for operation and maintenance activities. It is recommended that the Responsible Entity uses a Mobile Device Management (MDM) application or similar technology for its business, including email communication, calendar, data storage, and other activities.

R.10 The Responsible Entity shall maintain list(s) of Employees with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets

Regulation 6 Secure System Architecture

R.1 The Responsible Entity shall work out based on risk analysis, the necessary cyber security requirements in the System Architecture, during early planning phase**.**

R.2 The Responsible Entity shall design the entire system and its individual components so as to ensure cyber secure operations with minimal requirement of security hardening in the operation phase. Deliberate attacks and un-authorised actions shall be explicitly taken into account, while any repercussions arising from a security incident/event shall be minimized by the inherent design of systems.

Note:

It is recommended that the Secure System Architecture should be based of following principle:

1) Minimal need to know principle: Each resource/system and each user is only assigned the right needed to execute the function for which they have been authorised. Applications and network services, for example, are not run under administrator privileges, but only with the bare minimum of required system access right.
2) Defence in depth principle: Security risks are not tackled via single protection measures, but limited through the implementation of staggered multi-level and complementary security measures.
3) Redundancy principle: The entire system is designed to ensure that the failure of individual components does not impair security related functions. The secure system's design shall lower the likelihood and impact of issues caused by unrestricted request for systems resources such as e.g. main memory (RAM) or network bandwidth (so called resources consumption or DoS attack).

R.3 The Responsible Entity shall establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment and same for its OT/ICS environment. The Responsible Entity shall conduct regular enforcement checks to ensure that the baseline standards are applied uniformly.

Regulation 7 Cyber Crisis Management Plan(C-CMP)

R.1 The Responsible Entity shall prepare a Cyber Crisis Management Plan and submit to the sectoral-CERT for review with intimation to Ministry of Power/Authority. Before implementation of the C-CMP, the Responsible Entity shall get the C-CMP along with comments of sectoral-CERT vetted by CERT-In and finally get approved from Board of Directors.

R.2 The Responsible Entity shall review C-CMP at least annually. The CISO shall ensure that all changes are made in C-CMP only after the due approval of Board of Directors. The changes made in C-CMP must be communicated to all the concerned Personnels of the Responsible Entity, through a verifiable means.

Regulation 8 Cyber Risk Assessment and Mitigation Plan

R.1 The Responsible Entity shall document in its Cyber Security Policy, a Cyber Risk Assessment and Mitigation Plan approved by Board of Directors.

R.2 The Cyber Risk Assessment and Mitigation Plan shall be drawn upon the best practises being followed globally in the Power Sector. It shall contain a clearly defined the risk assessment matrix for both IT and OT environment and the latest modified risk acceptance criteria adopted by the Responsible Entity.

R.3 The Cyber Risk Assessment and Mitigation Plan shall be capable to demonstrate that repeated cyber security risk assessment delivers consistent, valid and comparable results.

R.4 ISD shall carry out Cyber Risk Assessment as per periodicity stipulated in the Cyber Risk Assessment and Mitigation Plan. Based upon the Cyber Risk Assessment report, ISD shall identify and characterise the inherent and/or residual risks within the Critical System and shall update the Mitigation Plan to minimize the residual risks.

R.5 ISD shall review, at least once in a Quarter, the risk assessment matrix and the risk acceptance criteria. For more effective implementation of Cyber Risk Assessment and Mitigation Plan, the risk assessment and mitigations measures exercised in the previous quarters shall be analysed in these Quarterly reviews.

Regulation 9 Personnel Risk Assessment

R.1 The Responsible Entity shall have a documented Personnel Risk Assessment procedure which shall be in accordance with the prevailing law of land and shall be subject to the latest collective bargaining unit agreements, for Employees having authorized cyber or authorized unescorted physical access. A Personnel Risk Assessment shall be conducted pursuant to that procedure within thirty days of such Employee(s) being granted such access.
R.2 The Responsible Entity shall subject all Employees and outsourced staff such as employees of service and utility providers, who have authorized access to the Critical Systems, networks and other computer resources, to the stringent supervision, monitoring and access restrictions. The Responsible Entity may implement the User and Entity Behaviour Analytics tools (UEBA) for combating cyber threats.
R.3 The Responsible Entity in compliance to the provision of Cyber Security Policy shall include in the Terms and Condition of Employment the requirement of periodic risk assessment of an Employee for grant of access to the Cyber Assets.
R.4 The Responsible Entity to mitigate threats from insiders, shall conduct background screening/checks as per Personnel Risk Assessment procedure, of every new Employee. Similar checks for risk assessment shall also be conducted at regular intervals on all Employees having access to the Critical System throughout their employment.
R.5 The Responsible Entity shall document in its Cyber Security Policy processes and controls to mitigate risks related to employee(s) terminating employment or changing responsibilities.
R.6 The Responsible Entity shall make every Employee sign an undertaking to protect the Confidentiality, Integrity and Availability of the Critical System and sensitive information owned and operated by the Responsible Entity.

Regulation 10 Change Control and Configuration Management

R.1 The Responsible Entity shall frame a comprehensive policy on Change Control Management that explicitly considers cyber risks, in terms of residual cyber risks identified both prior to and during a change, and of any new cyber risk created postchange
R.2 The policy on Change Control Management shall detail the supporting Configuration Management activities, e.g. to identify control and document all changes to hardware and software components of Critical System and the same shall be reviewed for relevancy and impact (business, technical and financial) by the Responsible Entity.
R.3 The Responsible Entity shall ensure that for any planned change, at minimum the policy on Change Control Management shall mandate:

1) A description of the proposed change,
2) The risk the system shall be exposed to in implementing the change.
3) Test procedure(s) and roll-out-plan and fall back plan,
4) Time & duration for testing and change,

5 Report on testing carried out in a non-productive environment,
6) Result from commissioning,

R.4 The Responsible Entity shall ensure that any configuration changes of a cyber asset, hardware or software, shall be approved before implementation of the change. The changes to be performed shall follow the accepted engineering practise for testing and according to the change control management.
R.5 The Responsible Entity shall ensure that any software change and/or update shall be controlled where available, with version control and/or supporting documentation.

R.6 The Responsible Entity shall ensure that fall-back procedure for aborting and recovering from unsuccessful changes shall be available and/or communicated.

R.7 CISO shall record the details of all emergency changes made along with reasons.

R.8 The configuration details of Critical System shall be current, and shall not be kept in the same secure environment or better than that of the cyber asset, and may be kept on the device if a backup device is in place.

R.9 The Responsible Entity shall ensure that the decommissioning of any cyber asset shall follow only after verifying that the cyber assets is no longer required or an upgraded/replacement has been/is being installed. The decommissioning process shall include the removal of software and information available from the cyber assets. Sensitive software and information shall be securely removed.

R.10 The Responsible Entity shall ensure that the use of live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place.

Regulation 11 Emergency Concept and Recovery Plan

R.1 The Responsible Entity shall identify and evaluate relevant emergency crisis scenarios as part of a business emergency and continuity management. To this end functions and application shall be classified according to their importance for business processes with particular attentions to a secure operational management. For the identified scenarios, emergency concepts and recovery plans shall be developed. The system design shall also be factored in the defined maximum down time and recovery periods, stated in the emergency concept.

R.2 The supplier shall provide documented and tested procedures and recovery plan including expected restoration times for relevant emergency and crisis scenarios, after relevant system updates. This documentation and these procedures shall be updated and retested as part of the approval process for Change Control Management.

R.3 The Responsible Entity shall ensure that wherever services from the suppliers are required for recovery and emergency operations, this shall be mentioned in the Agreement or in the Contract signed with the Supplier.

R.4 The Responsible Entity shall document Recovery Plan(s) for every Critical System in the C-CMP. Recovery Plan(s) shall be based upon lessons drawn during handling of any cyber incident or mock drill exercises and shall be regularly updated to remove the identified shortcoming(s). Changes in the Recovery Plan shall be made in line with policy on change control management.

R.5 The Responsible Entity shall communicate the updated Recovery Plan(s) to all its Employees responsible for implementation of C-CMP.

ISO/IEC 27002:2013/20719:2017, 17.1.1, 17.2.1

Regulation 12 Cyber Security Audit

R.1 The Responsible Entity shall document the implemented Information Security Management System (ISMS) covering all its Cyber Assets.

R.2 The Responsible Entity shall facilitate a comprehensive cyber security audit two times a year, first audit from April to September and second audit from October to March. The audit should commence immediately after the completion of the audit period and the auditor should submit the report within 6 weeks from commencement of the audit

R.3 The Responsible Entity through a CERT-In Empanelled Cyber Security OT Auditor, shall get their IT as well as OT System audited at least once in every 6 (six) months and shall close all critical and high risk vulnerabilities within a period of one month and medium as well as low risks non-conformity before the next audit. Immediate closure of non-conformance, based on the criticality is recommended. Effective closure of all non-conformities shall be verified during next audit.

R.4 The Cyber Security Audit shall be as per ISO / IEC 27001 along with sector specific standard ISO/IEC 27019, IS 16335 and other guidelines issued by appropriate Agency if any. These mentioned standards shall be current with all

amendments if any and in case if any standard is superseded, the new standard shall be applicable. R.5 ISD shall place the audit report and compliance status of the same before the Board of Directors for review. The ISD shall implement the corrective actions suggested during review taken by the Board of Directors and shall submit to the Board of Directors, regular updates on the reduction in no of non-compliances being observed subsequently during internal and externals cyber audits. The audit reports along with action taken report on reported non-conformances shall be submitted by the ISD to CISO-MoP as well as sectoral CERT within one month of submission of the report by the auditor.

R.6 The Responsible Entity shall change the Cyber Security OT Auditor every year at least, if the Auditing agency is not a government organization.

R.7 The CISO shall ensure that Responsible Entity has all the required systems and documents in place, as mandated in base line cyber security audit directive of
NSCS.

Regulation 14 Electronic Security Perimeter(ESP)

R.1 The Responsible Entity shall ensure that every Cyber Asset of the Critical System resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R.2 Access points to the Electronic Security Perimeter(s) shall also include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R.3 For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R.4 Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R.5 The Responsible Entity shall manage electronic access to Cyber Assets by specifying a controlled Electronic Security Perimeter, to protect Cyber Assets against compromise, that could lead to mis-operation or instability in the Power Supply System.

R.6 Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be also be identified and protected.

R.7 The Responsible Entity shall follow procedure of identifying “Electronic Security Perimeter” in case of distributed and/or hybrid information infrastructure, as per NERC CIP 005 / IS 16335 (as amended from time to time).

R.8 The Responsible Entity shall perform a cyber Vulnerability Assessment of the electronic Access Points to the Electronic Security Perimeter(s) at least once in every 6 (six) months and/or after any change in security of system architecture.

R.9 The Responsible Entity shall ensure that all critical, high and medium risk vulnerabilities identified upon cyber vulnerability assessment shall be closed and verified for the effective closure.

R.10 There shall be a separation (logical or possibly physical) between communication flows used to control and configure the network and application communication flows used to perform the actual work by the Responsible Entity. Use of separation VLAN for configuration and control and data communication between application would be an example strategy.

R.11 The Responsible Entity shall implement mechanisms (e.g., failsafe, load balancing, hot swap) to achieve resilience requirements in normal and adverse situations. Islanding mechanisms and other isolation techniques shall be implemented for resilient function and graceful degradation of service.

Regulation 15 Co-ordination with NCIIPC for cyber security of Protected System

R.1 The Responsible Entity shall co-ordinate with NCIIPC in regard to identification of CIIs and notification of some these CIIs as Protected System. In accordance with the mandate of NCIIPC to protect CIIs against cyber terrorism, cyber warfare and other threats and to maintain situational awareness, NCIIPC would need information, the same shall be furnished by the Responsible Entity as and when requested.

R.2 The Responsible Entity should collaborate/consult with Central Electric Authority (CEA), National Critical Information Infrastructure Protection Centre (NCIIPC) of
National Technical Research Organization (NTRO), Government of India, CERTIN etc. towards protection of critical assets and infrastructure and enhanced business continuity.

Regulation 16 Patch Management

The Responsible Entity shall document for all system components in detail the patch management procedures i.e. the procedure for security patch installation and uninstall or rollback and shall ensure that it includes the identification, categorization and prioritization of security patches.

R.2 Processes executed as part of this patch management procedure should meet recognised operating and service management standards (like COBIT, ITIL etc.)

R.3 The Responsible Entity shall establish an implementation timeframe for each category of security patches to implement security patches in a timely manner.

R.4 The Responsible Entity shall verify the integrity of security patches and updates using a cryptographic mechanism.

R.5 The Responsible Entity shall perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems. Fall back, rollback options in case of faulty patches or failed tests should be designed to facilitate a fast and easy return to the latest functional version and configuration test.

R.6 The installations of security and firmware updates for process related components (e.g. Controllers, PLCs, field units, protection devices) might require a facility shutdown, e.g. during a revision. Ideally, such components should be implemented and installed in a way that allows for on location patching with minimal testing efforts and without removal of the actual component.

R.7 The Responsible Entity shall ensure that Patch installations and un-install do not occur automatically.

R.8 The Responsible Entity shall authorise through written instruction(s) the concerned Employee or the nodal officer of the service provider engaged, to install the security patches and updates. Further all installations, uninstall shall be recorded in a transparent and tamper proof way within the system

R.9 The supplier shall ensure that the security updates and patches are available for all system components throughout the entire contractually stipulated operating timeframe. Where the supplier does not provide entire systems, he shall indicate the necessary processes and requirements to install security patches and other updates on the third party components used by the system.

R.10 Where no security patch is available to address a vulnerability the Responsible Entity shall ensure that controls are instituted to reduce any risk posed by such vulnerability to such a system and even in this case relevant security solution must be implemented in a time bound manner.

R.11 The Responsible Entity shall ensure that on each patch supplier has done clear labelling and provided version number. Where patches need specific firmware versions, compliance shall be verified and ensured separately by the Responsible Entity.

ISO/IEC 27002:2013/27019:2017 12.5.1, 12.6.1

Regulation 17 Application Security and Testing

R.1 The Responsible Entity shall ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests should cover Functionality, Security controls and system performance under various stress-

load scenarios and recovery conditions. For ICS/OT systems, testing of applications and patches at surrogate test-bed designated by Ministry of Power shall be carried out before putting them into Power Supply System.
The Responsible Entity shall ensure that no application should be introduced in the production environment without adequate testing. Certificates on testing of security features of software should be mandatorily provided.
R.3 Traditional isolated testing implicitly assumes that all other systems operate as usual. Removing this hypothesis helps the Responsible Entity to identify plausible complexities, dependencies and weaknesses that may have been overlooked in its recovery plans. Accordingly, testing shall include all scenarios that cover breaches affecting multiple portions of the Responsible Entity's ecosystem. For example, for OT/ICS security testing, breach of IT system that can leak into the OT/ICS should be considered as a plausible scenario.
R.4 The Supplier needs to document both the necessary test cases and the expected results of a successful test run (test book, depending on system criticality, functional testing might require a **Buyer** specific test system at the supplier's location and additional testing at the location of Responsible Entity).

Regulation 18 Maintenance and Testing

R.1 The Responsible Entity shall establish and manage a baseline of network operations and expected data flows for users and systems.
R.2 The Responsible Entity shall perform on their own or through Vendor from Trusted Source, the System Identification & Trusted System (SITS) Scanning, which shall include but not limited to the following: - 1) Match each open port to a service and protocol.

2) Identify server uptime to latest patch releases.
3) Identify the application behind the service and the patch level using banners or finger-printing.
4) Verify the application to the system and the version.
5) Locate and identify service remapping or system redirects.
6) Identify the components of the listening service.
7) Use UDP-based service and Trojan requests to all the systems in the network
8) exhaustive Malware Scanning for hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.
9) Lockout Testing to mitigate the brute force attack etc.
10) Password Cracking to mitigate the brute force attack, cryptographic attack etc.

R.3 The Responsible Entity shall carry out Integrity testing to check system files, applications configurations files and applications for integrity, for example through cryptographic checksums
R.4 The Responsible Entity shall maintain all testing and maintenance records as per the document retention policy.
Requirement: ISOIEC 27002:2013/27019:2017 12.5.1., 14.2.1, 14.2.4

Regulation 19 Phasing out of Legacy System

R.1 As the life cycle of the Equipment/System deployed in Power Supply System is longer than that of IT Systems deployed therein, the Responsible Entity shall ensure that all IT technologies should have the ability to be upgraded.
R.2 ISD shall draw the list of all communicable devices nearing end life or left without support from OEM. The CISO shall firm up and put up the replacement plan for equipment/systems identified to be phased out, for approval before the Board of Directors.
The Responsible Entity shall regularly conduct vulnerability assessment to detect security vulnerabilities in both IT and IT/ICS environment. The Responsible Entity shall also carry out periodic penetration tests, at least twice in a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.

R.4 The Responsible Entity shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces.
R.5 The CISO shall ensure that till devices nearing end life or left without support from OEM are not replaced, their cyber security is hardened and ensured, in consultation with the OEM or alternate Supplier(s).
R.6 In addition to the periodic vulnerability assessment and penetration testing conducted to evaluate security posture, the Responsible Entity shall also conduct periodic table-top exercises, mock drills, etc. to improve its preparedness to handle cyber breach/incident. Such exercises should be followed-up with a detailed review by ISD.
R.7 The Responsible Entity shall document in their Cyber Security Policy a Standard Operating Procedure for safe and secure disposal of outlived or legacy devices.
R.8 The Responsible Entity shall frame suitable policy for disposal of the storage media and systems. The data/information on such devices and systems should be removed/destroyed as per set policy by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.
R.9 The Responsible Entity shall ensure that before disposing of a telecommuting client device or remote access server, all sensitive data has been removed.
R.10 The Responsible Entity shall ensure that the decommissioning and disposal of legacy hardware and software does not create system vulnerabilities by using processes to:

1) remove sensitive information from and prompt disposal of decommissioned hardware and software; and
2) run Vulnerability Assessment and Penetration Testing (VAPT) to reassess vulnerability and risk assessments whenever legacy systems are replaced with more modern systems.
3) remedial actions shall be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

ISO/IEC 27002:2013/27019:2017 12.6.1, 14.2.7

Supply Chain Risk Management

Regulation 20: Supply Chain Cyber Security Risk Management Plan

R.1 The Responsible Entity shall have documented supply chain cyber security risk management plan(s) for high and medium impact Cyber Systems. The plan(s) shall include:

1) One or more process(es) used in planning for the procurement of Cyber Systems to identify and assess cyber security risk(s) to the Power Supply System from vendor products or services resulting from:
   a) procuring and installing vendor equipment and software; and
   b) transitions from one vendor(s) to another vendor(s).
2) One or more process(es) used in procuring Cyber Systems that address the following, as applicable:
   a) Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
   b) Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
   c) Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
   d) Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;
   e) Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the Cyber System; and
   f) Coordination of controls for

(i) vendor-initiated Interactive Remote Access, and
(ii) system-to-system remote access with a vendor(s)

R.2 ISD shall ensure implementation of supply chain cyber security risk management plan(s) and shall record all instances of violation for appraisal of Board of Directors.

R.3 ISD shall review at least once in a year supply chain cyber security risk management plan(s) and shall seek approval of Board of Directors for necessary changes required to ensure that violations as recorded in R.2 are not repeated, if they were due to genuine shortcomings in the plan.

Regulation 23 Vendor Management

R.1 The Responsible Entity shall put in place a vendor management programme to ensure that vendors meet security requirements and that appropriate safeguards are implemented. The Responsible Entity is encouraged to adopt industry standards (e.g. SOC 2, SSAE 18) as well as independent audits. The programme shall inter alia contain established procedures for terminating or replacing vendors, including cloud-based service providers.

R.2 The Responsible Entity shall understand all contract terms including rights, responsibilities, expectations and other specific terms and ensure that all parties have the same understanding of how risk and security is addressed. The Responsible Entity is expected to understand and manage the risks related to vendor outsourcing, including the vendor's use of cloud-based services.

R.3 The Responsible Entity shall monitor the relationship with its vendor to ensure that the vendor continues to meet security requirements and to be aware of changes to the vendor's services or personnel.

R.4 The Responsible Entity shall implement IEC 62443 for Monitoring and Detection. Of Cyber risk to their ICS/OT infrastructure from Vendors/Suppliers.

R.5 The Responsible Entity shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.

R.6 The Responsible Entity shall ensure that the information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. This shall inter alia include the following functions: 1) The network is monitored to detect potential cybersecurity events in real time

2) The physical environment is monitored to detect potential cybersecurity events
3) Personnel activity is monitored to detect potential cybersecurity events in real time
4) Malicious code is detected
5) Unauthorized mobile code is detected
6) External service provider activity is monitored to detect potential cybersecurity events
7) Monitoring for unauthorized personnel, connections, devices, and software is performed
8) Vulnerability scans are performed

R.7 The Responsible Entity shall put in place necessary systems for monitoring the activities of the external service provider to detect potential cybersecurity events.

R.8 In order to ensure high resilience, high availability and timely detection of attacks on systems and networks, a Responsible Entity should implement suitable mechanism to monitor capacity utilization of its critical systems and networks. To that effect, a Responsible Entity shall ensure the following:

1) A baseline of network operations and expected data flows for users and systems is established and managed.
2) Detected events are analysed to understand attack targets and methods
3) Event data are collected and correlated from multiple sources and sensors

4 Impact of events is determined

5) Incident alert thresholds are established
6) Sensor measurements traditionally used for control should be also monitored for anomalies and alert generation

R.9 The Responsible Entity shall ensure that monitoring for unauthorized personnel, connections, devices, and software is performed constantly.

R.10 Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual sensor readings, or control system anomalies.

R.11 The Responsible Entity's protective controls should enable the monitoring and detection of anomalous activity across multiple layers of the Responsible Entity infrastructure. Controls should be implemented in a way that will assist in monitoring for, detecting, containing and analyzing anomalous activities, if protective measures fail. As a cyber-attack typically progresses in a sequence of stages before attaining its end objective, Responsible Entity' s should also apply approaches that enable them to delay or disrupt the attackers' ability to advance within the attack sequence.

Incident Management

Regulation 24 Disturbances or unusual occurrences, suspected or determined to be caused by sabotage.*

R.1 The Responsible Entity shall have procedures for the recognition of and for making their operating Personnel aware of sabotage events on their facilities and multi-site sabotage affecting the functioning of Critical System.

R.2 The Responsible Entity shall provide its Personnel with sabotage response guidelines, including Personnel to contact, for reporting disturbances due to sabotage events.

R.3 The Responsible Entity shall designate Personnel for the communication of information concerning sabotage events to the sectoral CERT as well as CERT-In.

R.4 The Responsible Entity shall establish communications contacts, as applicable, with National Cyber Security Co-ordinator or CERT-In (MeitY) and develop reporting procedures as appropriate to their circumstances.

R.5 The Responsible Entity shall have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative process. In this regard, the **Responsible Entity** shall establish relevant system logging policies that include the types of logs to be maintained and their retention periods. The Responsible Entity shall take appropriate steps so that investigations can still be performed post-event to the extent possible, e.g. through preservation of necessary system logs and evidence.

***Sabotage e.g. can be a forced intrusion in un-manned/ manned facility and taking control of operation of Critical System through a communicating device.**

Regulation 25 Sabotage Reporting

R.1 The Responsible Entity shall incorporate procedure for identifying and reporting of sabotage in their Cyber Security Policy, within 30 days from notification of the Guideline or grant of licence to the Responsible Entity under the appropriate provisions of Act.

R.2 The CISO shall be liable for reporting of identified sabotage(s) as per procedure laid in the Cyber Security Policy of the Responsible Entity.

R.3 The CISO shall prepare a detailed report on disturbances or unusual occurrences, identified, suspected or determined to be caused by sabotage in the Critical System of the Responsible Entity, and shall submit the report to the Sectoral CERT as well as CERT-In within 24 hours of occurrence.

R.4 The CISO shall submit to National Critical Information Infrastructure Protection Centre (NCIIPC) within 24 hours of occurrence the report on every sabotage classified as cyber incidents(s) on "Protected System".

R.5 The CISO shall take custody of all log records as well as digital forensic records of affected Cyber Assets, Intrusion Detection System, Intrusion

Protection System, SIEM and shall preserve them for at least 90 days and shall make them available as and when called upon for investigation by the concerned Agencies.

Regulation 26 Incident Response

R.1 The Responsible Entity shall develop a risk-assessed incident response plan for various scenarios including denial of service attacks, malicious disinformation, ransomware attacks, key employee succession, as well as extreme but plausible scenarios. The Responsible Entity shall take into consideration the past cybersecurity incidents and current cyber-threat intelligence in developing business continuity plans and policies and procedures. The Responsible Entity shall establish and maintain procedures that include: 1) timely notification and response if an event occurs

2) a process to escalate incidents to appropriate levels of management, including legal and compliance functions
3) communication with key stakeholders.

R.2 Alerts generated from monitoring and detection system should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such potential incident of cyber-attack or breach, mitigate its effect and eradicate the incident. The response activities should be coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

R.3 The response and recovery plan of a Responsible Entity shall aim at timely restoration of systems affected by incidents of cyber-attacks or breaches. The recovery plan shall be in line with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified in the Cyber Security Policy.

R.4 The Responsible Entity shall conduct response and recovery planning and testing with suppliers and third-party providers. The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of cyber security mechanism.

Regulation 27 Cyber Security Resilience Policy

R.1 The cyber security resilience policy of the Responsible Entity shall include the following functions to discern, assess and manage cyber security risk associated with processes, information, networks and systems.

1) 'Identify' critical IT/OT/ICS assets and map risks associated with each asset,
2) 'Protect' assets by deploying suitable controls, tools and measures, especially implementation of controls listed in IEC 62443 Standards
3) 'Detect' incidents, anomalies and attacks through appropriate monitoring tools / processes, deployed at Security Operation Centre (SoC) or critical IT/OT/ICS assets are managed at CERT-In CSK
4) 'Respond' by taking immediate steps after identification of the incident, anomaly or attack, including communication to appropriate regulatory authorities, CERT-IN, and NCIIPC
5) 'Recover' from incident through incident management, disaster recovery and business continuity framework.

Regulation 28 Recovery Management

R.1 The Responsible Entity shall establish process to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

R.2 The Responsible Entity shall endeavour to continuously improve response activities by incorporating lessons learned from current and previous detection/response activities. Any incident of loss or destruction of data or systems should be thoroughly analysed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

R.3 The Responsible Entity shall also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan. The response and recovery planning and testing should be conducted with suppliers and third-party providers.

R.4 In the event of a successful cyber-attack that compromises the integrity of the Responsible Entity's data, a successful recovery may require obtaining uncorrupted data from third parties and/or participants. The Responsible Entity shall set up datasharing agreements with relevant third parties or participants in advance in order to enable such uncorrupted data to be received in a timely manner once a successful cyber-attack has been identified. Because Responsible Entity's systems and processes are often interconnected with the systems and processes of other entities within its ecosystem, in the event of a large-scale cyber incident it is possible for a Responsible Entity to pose contagion risk (ie, propagation of malware or corrupted data) to, or be exposed to contagion risk from, its ecosystem(for example from or to Load Dispatch Centres). The Responsible Entity shall work together with its interconnected entities to enable the resumption of operations (the first priority being its critical services) as soon as it is safe and practicable to do so without causing unnecessary risk to the wider sector or further detriment to financial stability.
R.5 The Responsible Entity shall ensure that the recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
R.6 The Responsible Entity shall endeavour to improve the recovery planning and processes by incorporating lessons learned into future activities and that the recovery strategies are updated from time to time.
R.7 The Responsible Entity shall communicate the recovery activities to the internal and external stakeholders.

Regulation 29 Cyber Security Incident Report and Response Plan

R.1 The CISO of the Responsible Entity shall report all Cyber Security Incidents, classified as reportable event, as per procedures and in the formats prescribed by CERT-In.
R.2 Root cause analysis for all reportable event shall be carried out with the corrective action plan, so as to ensure any re-occurrence of such event can be managed with ease.
R.3 The Responsible Entity shall mandatorily define in their Cyber Security Policy, criteria(s) identified on the basis of impact analysis, for declaring the occurrence of Cyber Security Incident(s) in the System of Responsible Entity as a Cyber Crisis.
R.4 The Responsible Entity shall mandatorily designate and empower the Personnel and his/her standby, by name and designation with their contact details made available in the Cyber Crisis Management Plan, to declare the incident(s) to be a Cyber Crisis.
R.5 The CISO shall ensure that during any Cyber Incident, ISD shall monitor minutely and record every details of cyber security events and incidents in both IT and OT infrastructure of the Responsible Entity.
R.6 The CISO shall ensure that each cyber incident is handled strictly as per Cyber Security Incident Response Plan as detailed in Cyber Crisis Management Plan.
R.7 The efficacy of the Cyber Security Incident Response Plan should be tested annually through mock drill(s) carried out as simulation exercise(s), if feasible for Responsible Entity or as a table top exercise(s) with wider participation of their employees, in consultation with CERT-In and sectoral CERT and in case if any shortcomings observed make suitable changes in the Cyber Security Incident Response Plan.
R.8 The CISO of the Responsible Entity shall compile details of incident detection, incident handling, learnings from incident and damage claims made if any and shall report to CERT-In as well as ISAC-Power.

Regulation 30 Physical security

R.1 The Responsible Entity shall identify and protect Transmission lines and Transmission substations, and their associated primary control centres, that if rendered inoperable or damaged as a result of a physical attack could result in wide spread instability, uncontrolled separation, or Cascading within an Interconnection.
R.2 The Responsible Entity shall ensure that the perimeter of the Critical System is physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access

systems, mantraps, bollards, etc. where appropriate. The Responsible Entity shall ensure that there is no time lag in the CCTV recordings.

R.3 Physical access to the Critical Systems (especially OT and ICS) should be restricted to a minimum. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that the outsourced staff/visitors are always accompanied by authorized employees.

R.4 Physical access to the Critical Systems should be revoked immediately if the same is no longer required.

Regulation 31 Cyber Security Training.

R.1 The Responsible Entity shall establish, maintain, and document an annual cyber security training program for Employees having authorized cyber escorted or unescorted physical access to Critical Cyber Assets.

R.2 The Responsible Entity shall ensure that all Employees having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

R.3 Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

1) The proper use of Critical Cyber Assets;
2) Physical and electronic access controls to Critical Cyber Assets;
3) The proper handling of Critical Cyber Asset information; and,
4) Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R.4 The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R.5 The cyber security training program shall be reviewed annually, and shall be updated whenever necessary. Effectiveness of the training shall be evaluated and records maintained.

R.6 Cyber Security Training Program must cover following: 1) User authentication and authorization.

2) Cyber Security and Protection mechanisms of OT/ICS Systems.
3) Introduction to various standards i.e. ISO/IEC:15408, ISO/IEC:24748-1, ISO: 27001, ISO: 27002, ISO 27019, IS 16335, IEC/ISO:62443.
4) Training on implementation of ISO / IEC 27001 and awareness on IEC 62443. 5) Vulnerability Assessment in the Critical System.
6) Monitoring and preserving of logs of electronic access of Critical Cyber Assets. 7) Detecting cyber-attacks on SCADA systems
8) The handling of Critical System during cyber crisis.
9) Action plans and procedures to recover or re-establish normal functioning of Critical Cyber Assets and access thereto following a Cyber Security Incident.
10) Hands on SCADA operation at any Regional Load Dispatch Centre. 11) Handling of risks involved in procuring COTS Products.

R.7 The Responsible Entity shall ensure that all operation and maintenance Employees managing SCADA System shall undergo mandatory cyber security training immediately within 30 days from notification of these Regulations

R.8 Newly hired/current Employees of the Responsible Entity shall not have access to Critical Cyber Assets prior to the satisfactory completion of cyber security training programme from the designated Training Institute in India, except in specified circumstances such as an emergency.

R.9 The Responsible Entity shall ensure that its Employees and Employees of partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements. The Responsible Entity shall conduct periodic awareness and training programs for its Employees,

participants and intermediaries with regard to cyber security, situational awareness and social engineering.

R.10 The Responsible Entity shall give special focus to build awareness levels and skills of staff from non-technical disciplines and training of 'High-risk groups', such as those with privileged system access or in sensitive business functions.

R.11 The Responsible Entity shall ensure that Privileged users, Senior executives, cybersecurity personnel and third-party stakeholders understand their roles and responsibilities.

R.12 The Responsible Entity shall provide specific cybersecurity and resiliency training which inter alia should include:

1) phishing exercises to help employees identify phishing emails
2) preventive measures such as identifying and responding to indicators of breaches, and obtaining investor / vendor / employee confirmation if behaviour appears suspicious.
3) mobile device policies and effective practices to protect mobile devices.
4) OT/ICS Security and protection mechanisms
5) Training on IEC62443 implementation

R.13 The Responsible Entity shall ensure that its employees attend the training programme and continuously assess and evaluate the effectiveness of such training. The training programs should be updated from time to time based on cyber-threat intelligence

R.14 The Responsible Entity shall ensure that CISO and members of ISD shall be sent for special training programs in IT, OT and ICS security with suitable certification Periodic Audit.

Information Sharing and Data Security

Regulation 32 Security of Data

R.1 The Responsible Entity shall have a policy of encrypting all sensitive data when it is at rest on the device and on removable media used by the device. The creation and use of crypto graphic keys for encrypting remote data at rest should follow the same policies that the Responsible Entity has for other keys that protect data at rest.

R.2 The Responsible Entity shall ensure that the Data-in motion and Data-at-rest should be in encrypted form, on all the systems including but not limited to internet facing systems. Light-weight cryptography solutions may be utilized in time sensitive inter system communications.

R.3 The Responsible Entity shall ensure that the sensitive information, such as certain types of Personally Identifiable Information (PII)(e.g., personnel records, financial records, transaction records), that is stored on or sent to or from telecommuting devices should be protected so that malicious parties cannot access or alter it.

R.4 The Responsible Entity shall implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.

R.5 The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.

R.6 The Responsible Entity shall allow only authorized data storage devices through appropriate validation processes.

R.7 To avoid disaster due to ransomware attack, backup of all data, system, applications, encrypted credentials, firmware etc should be taken on a daily basis –based on the frequency of change of the type of information being backed up. Automated solution for restoration from backup should be implemented, and periodically tested.

R.8 All data sent to the employee/vendor/business partner through remote access should be covered by the 'Responsible Entity's data distribution and data retention policies.

R.9 The Responsible Entity shall put in place adequate safeguards to prevent printing, copying, pasting or saving information to personally owned computers, smartphones or tablets. Further, the PSO should have the ability to remotely clear data and content from a device that belongs to a former employee or from a lost device. Hardening of Hardware and Software.

R.10 Only hardened and vetted hardware / software should be deployed by a Responsible Entity. During the hardening process, the Responsible Entity should inter-alia ensure that:

1) default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipments / software
2) all removable media are protected, and their use restricted according to policy

R.11 All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports. All USB ports should be blocked on the machines on critical segments of the network.

R.12 The Responsible Entity shall ensure that the developer of the information system, system component or information system service enables integrity verification of software and firmware components through verifiable digital signature with verifiable digital certificates.

R.13 The Responsible Entity shall ensure that all types of telecommuting client devices (which inter alia include Personal Computers, laptops, smartphones and tablets) are secured. Depending on the device type and product type, the Responsible Entity shall provide guidance to device administrators and users (who are responsible for securing telecommuting mobile devices) on how they should be secured

R.14 Confidential data only be stored and transmitted encrypted. Confidential data might for example include log files passwords parameterisation data or confidential data to official regulation and relevant legislation.

R.15 The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Systems.

i) The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Systems information.

R.16 The Responsible Entity shall, at least annually, assess adherence to its Critical System information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

ISO/IEC 27002:2013/ 27019:2017, 10.1.1, 12.4.2, 13.1.2, 18.1.3

Regulation 33 Cryptographic Mechanism

R.1 While selecting cryptographic mechanism, CERT-In advisory shall be adopted. Only CERT-In approved mechanism and minimum key sizes shall be used that are considered secure for the foreseeable future according to state of the art technological knowledge. The supplier shall not use custom cryptographic algorithm. For particular filed application the IEC 62351 standard series defines clear requirement for supported cryptographic mechanism.

CERT-In may give directive and recommendations that need to considered state-of-art for hashing, signatures and encryption as well as related key sizes.

Where possible, the implementation of cryptographic mechanism should involve recognized libraries to avoid implementation errors. It might be advisable to use cryptographic hardware modules like a trusteed platform module(TPM) for key management and random number generation etc.

Requirement: ISO/IEC 27002:2013/27019:2017, 10.1.1, 10.1.2, 13.1.4, 18.1.5

Regulation 33 Use of cloud Services

R.1 Where cloud services are used the following requirement shall apply:

a) Agreements shall be made with the cloud service provider about security related processes for cloud infrastructure operations.
b) Functions for the control of CII & Protected system where manipulation could threaten the energy supply, shall not be realised in external cloud services.
c) Downtime of a cloud services access to this service shall not lead to significant restriction of the system defined basic function. Cloud services disruptions or outages shall also be considered in the emergency concept and restoration plans.
d) The following issues, especially requires binding agreement; Access authentication /authorization

ISO/IEC 27002:2013/27019:2017 15.1.1, 15.1.2, 15.2.1

Regulation 33 Cyber Incidence Reports

R.1 The Responsible Entity shall document a Privacy Policy to support compliance of cyber security activities with minimum data protection and privacy standards. 1) A process should be instituted to conduct a privacy review of the Responsible Entity's anomalous activity detection controls and Standard Operating Procedure (SOP) for monitoring of cyber security architecture. The Responsible Entity shall assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cyber security information sharing activities.

R.2 The Responsible Entity shall prepare regularly Quarterly Cyber Incidence Reports containing information on cyber-attacks and threats if any experienced and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/vulnerabilities/threats that may be useful for other Responsible Entities, should be submitted to Ministry of Power as well as NCIIPC. The hard copy of the report in sealed cover should be submitted by 5th of the next month of every Quarter.

R.3 The Responsible Entity shall share hard copy only of these reports in sealed cover with the MHA, Regulatory Bodies, National Cyber Security Co-ordinator, NCIIPC and CERT-in as well as SEBI as and when called upon in writing to do so, without holding back any part or concealing any detail.

R.4 Any data that can be used to identify a person or its behaviour directly of by association are considered personally identifiable data. Such data shall enjoy special protection to allow the affected person to exercise their right to information and decide for themselves who what where and when get to access their personal data.

R.5 Manufactures and suppliers are requested to supply the technical and organisational requirement of the existing protection regulation as operative functions of their products.

R.6 Individuals with cyber security-related privacy responsibilities should report to appropriate management and be appropriately trained. Steps should taken to identify and address the privacy implications of identity management and access control measures to the extent that they involve collection, disclosure, or use of personal information.

R.7 The Responsible Entity shall include applicable information from its privacy policies in cyber security workforce training and awareness activities. Service providers that provide cyber security-related services for the Responsible Entity shall be informed about the organization's applicable privacy policies

Regulation 34 Documentation and Retention Policy

R.1 The CISOs shall be the originator and custodian of all the controlled documents including Cyber Crisis Management Plan, Cyber Risk Assessment and Mitigation
Plan, Statement of Applicability of Controls, and compliance to Regulator's requirement.

R.2 The Responsible Entity shall ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs shall be maintained and stored in encrypted form for a time period not less than two (2) years.