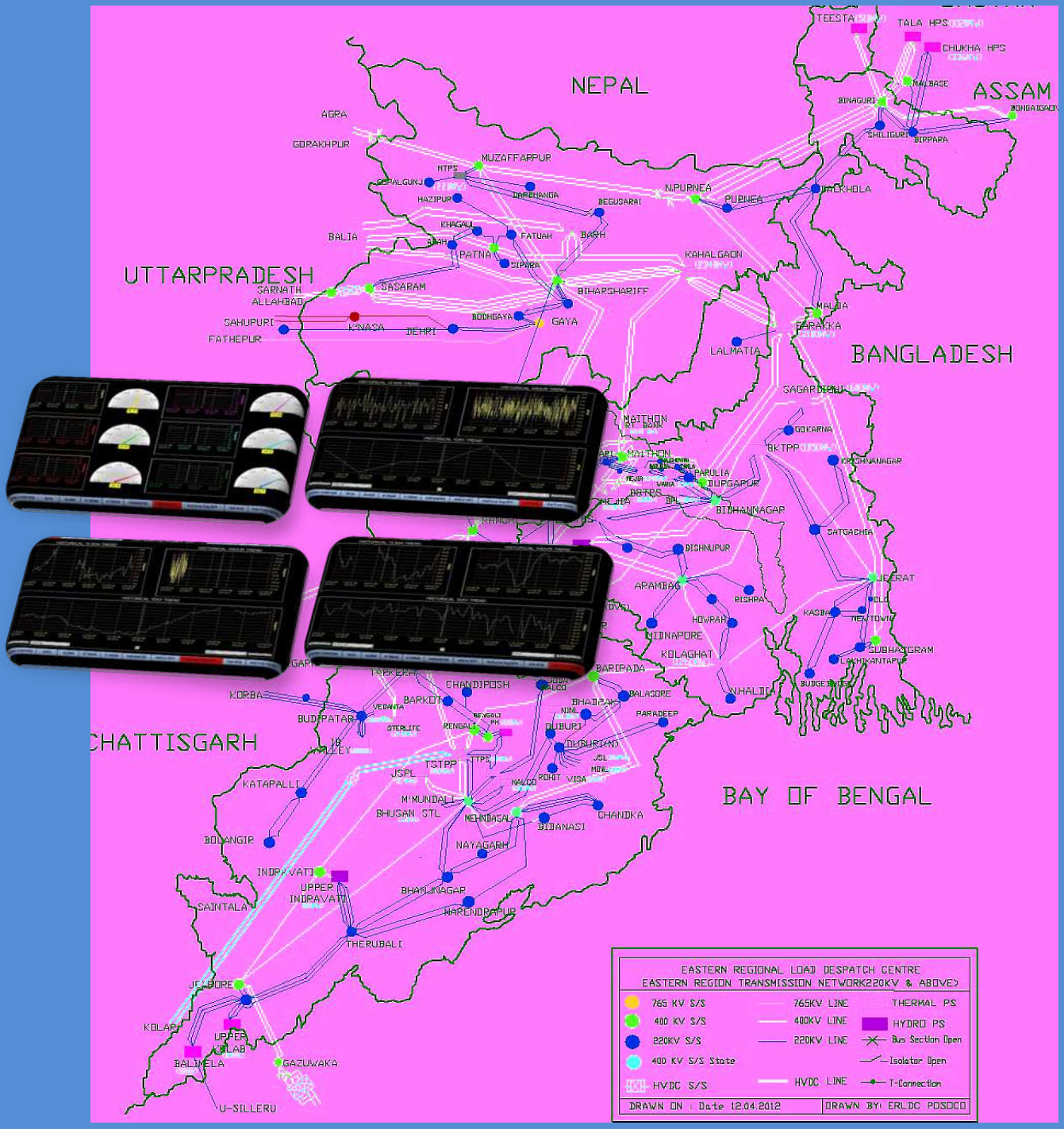
BID DOCUMENT

For

Implementation of Managed IT System Security Service and Network Threat Monitoring, Detection & Resolution Services

AT

Eastern Region Load Despatch Center



पावर सिस्टम ऑपरेशन कॉरपोरेशन लिमिटेड

POWER SYSTEM OPERATION CORPORATION LIMITED

पूर्वी क्षेत्रीय भार प्रेषण केन्द्र

Eastern Regional Load Despatch Centre

14 Golf Club Road, Tollygunge, Kolkata 700033

Government eProcurement System

eProcurement System Government of India

Published Corrigendum Details

Date : 22-Mar-2016 12:32 PM

Print

Organisation Chain :	Power System Operation Corporation Limited||ERLDC-Kolkata-POSOCO||Contracts and Materials Dept-ERLDC-POSOCO
Tender ID :	2016_POSOC_74027_1
Tender Ref No :	ERLDC/CNM/1119/AntiVirus etc./2016
Tender Title :	Implementation of IT Security and Network threat monitoring at ERLDC
Corrigendum Type :	Date

Corrigendum:1

Corrigendum Title	Corrigendum Description	Published Date	Document Name	Doc Size(in KB)
Extension of Bid submission and opening date	Extension of Bid submission and opening date	22-Mar-2016 12:30 PM	EXTENSIONLETTER.pdf	399.29

Critical Dates			
Publish Date	29-Feb-2016 12:00 PM	**Bid Opening Date**	01-Apr-2016 03:00 PM
Document Download/Sale Start Date	29-Feb-2016 05:00 PM	**Document Download/Sale End Date**	01-Apr-2016 12:00 PM
Clarification Start Date	29-Feb-2016 05:00 PM	**Clarification End Date**	31-Mar-2016 12:00 PM
Bid Submission Start Date	01-Mar-2016 05:00 PM	**Bid Submission End Date**	01-Apr-2016 12:00 PM
Pre Bid Meeting Date	10-Mar-2016 11:00 AM		

Details Before Corrigendum

Critical Dates			
Publish Date	29-Feb-2016 12:00 PM	**Bid Opening Date**	22-Mar-2016 03:00 PM
Document Download/Sale Start Date	29-Feb-2016 05:00 PM	**Document Download/Sale End Date**	21-Mar-2016 05:00 PM
Clarification Start Date	29-Feb-2016 05:00 PM	**Clarification End Date**	21-Mar-2016 12:00 PM
Bid Submission Start Date	01-Mar-2016 05:00 PM	**Bid Submission End Date**	21-Mar-2016 05:00 PM
Pre Bid Meeting Date	10-Mar-2016 11:00 AM		

POWER SYSTEM OPERATION CORPORATION LIMITED

Eastern Regional Load Despatch Centre

14 Golf Club Road, Tollygunge, Kolkata 700033

Implementation of Managed IT System Security Service and Network Threat Monitoring, Detection & Resolution Services at ERLDC.

(E-TENDERING)

CONTENTS

DOC Reference No. :	Issue Date:
ERLDC/C&M/1119/Antivirus etc/2016	**February 25, 2016**

AT A GLANCE

SCOPE OF WORK

Implementation of Managed IT System Security Service and Network Threat Monitoring, Detection & Resolution Services at ERLDC.

PRICE OF BID *Rs.1250/-*

DATES TO REMEMBER

Description	Date
Downloading of BID Document	from 17:00 Hrs. 29.02.2016 to 10:00 Hrs. 21.03.2016
Last Date of submission of EMD/Bid Security, Integrity Pact, Bid Price, in original (Hard Copy)	Upto 17:00 Hrs of 18.03.2016 on all working days.
Last Date of Submission of BID	17:00 Hrs., 21.03.2016
Date of Opening of First Envelop	15:00 Hrs., 22.03.2016

BID SECURITY *Rs.46,800/-*

ESTIMATED COST *Rs.23,40,025/- including tax*

BID DOCUMENT SECTIONS

Section I IFB	Invitation for BID
Section II ITB	Instruction to Bidder
Section III GCC	General Condition of Contract
Section IV SCC	Special Condition of Contract
Section V TS	Technical Specification & Scope of work
Section VI FORMS	Forms & Formats

ADDRESS FOR CORRESPONDENCES

Eastern Regional Load Despatch Centre, *Power System Operation Corporation Limited*
14 Golf Club Road, Tollygunge Kolkata 700033
(m) +91 9433041848 e-mail: skmukh@hotmail.com

पावर सिस्टम ऑपरेशन कॉरपोरेशन लिमिटेड

POWER SYSTEM OPERATION CORPORATION LIMITED

पूर्वी क्षेत्रीय भार प्रेषण केन्द्र

Eastern Regional Load Despatch Centre

14 Golf Club Road, Tollygunge, Kolkata 700033

INVITATION FOR BID (IFB)

For

IMPLEMENTATION OF MANAGED IT SYSTEM SECURITY SERVICE

And

NETWORK THREAT MONITORING, DETECTION AND RESOLUTION SERVICES

At ERLDC

SECTION - I

DOC Reference No. : ***ERLDC/C&M/1119/Antivirus etc/2016***	Issue Date: **February 25, 2016**

Table of Contents

1. TITLE OF THE PROJECT

Implementation of Managed IT System Security Service and Network Threat Monitoring, Detection & Resolution Services at ERLDC.

2. GENERAL INFORMATION

A "Single Stage Two Envelops" bidding procedure will be adopted and will proceed as detailed in the Bidding Documents.

The bid shall be submitted in two envelops Viz.

Envelop – 1 (Technical Qualification): Containing the following in separate envelops:

a) Compliance of qualifying criteria & documentary evidences for the same (refer para 6.0 for QR, Section -VI for relevant forms & formats)

b) Integrity Pact. **(in duplicate duly signed and sealed by the bidder on a non judicial stamp paper of Rs. 100/-)**

c) **Bid security of Rs.46,800/-** in form of DD / Bank Guarantee / Banker Cheque (refer Clause 10 of ITB)

Envelop – 2 (Price Bid) containing commercial offer along with the bidding schedule as enclosed in Section –VI.

Technical Part shall be opened first. Bids satisfying the pre-qualifying requirement only shall be evaluated for commercial offer. Please ensure that your bid is submitted well in time on or before the due date and time of opening. **Late tenders are not accepted**. POSOCO would not be responsible for any delay whatsoever.

BIDs shall be submitted as per prescribed formats duly filled in & attached. (Section –VI **– Forms for Formats details.)**

For more details refer to section – II Instruction to bidder (ITB).

All Bids must be accompanied with a bid security of INR 46,800/-

Bids not accompanied with valid Bid Security in accordance with Clause 10 of ITB, shall not be entertained and will not be evaluated further.

Micro and Small Enterprises (MSEs) / Bidders registered with NSIC may also bid with documentary evidence. Tender fees and EMD shall be exempted for such bidders.

Location/Destination	ERLDC, Power System Operation Corporation Limited. 14 Golf Club Road, Tollygunge, Kolkata 700033
Validity	6 months from the date of opening of the bid.

Scope of work, Specification & BOQ

Scope of work is as per section – V Technical Specifications. BOQ enclosed in Section VI as forms and formats.

3. TERMS & CONDITIONS

3.1. Contract Performance Guarantee

As a contract performance security, the successful bidder, to whom the contract is awarded, shall be required to furnish contract Performance Guarantee (CPG) from (a) a public sector Bank or (b) from a schedule Indian Bank having paid up capital (net of any accumulated losses)of Rs. 100 crores or above (the latest annual report of the bank should support compliance of capital adequacy ratio requirement)or any foreign Bank or subsidiary of a foreign Bank with overall international corporate rating or rating of long term debt not less than A – (a minus) or equivalent by reputed rating agency in the prescribed format. The guarantee amount shall be equal to 10% of the contract price and it shall guarantee the faithful performance of the contract in accordance with the terms and conditions specified in the NIT document and specification. The contract performance guarantee shall be furnished within 28 days from the date of placement of order and shall be kept valid for a period of 90 days after the end of contract period of three years.

Alternatively

Security Deposit:-10% of the Billed amount of the successful bidder shall be deducted towards security deposit from all running/final bills towards faithful performance of contract. The amount so deducted shall be released 90 days after the end of contract period of three years subject to successful completion of contract and duly certified by the Engineer-in-Charge. The EMD submitted along with the Bid shall be released after deduction of security deposit.

3.2. Payment Terms

2.1 100% of the billed amount of the successful bidder, who opted for CPG shall be released within 15 days by e- payment after successful implementation of the job as certified by the Engineer- in -charge or by the CONSIGNEE at the Tollygunge premises of POSOCO. The payment will be released subject to submission of valid CPG.

Alternatively

90% of monthly billed amount shall be released within 15 days by e-payment after successful implementation of the job as certified by the Engineer- in -charge or by the CONSIGNEE at the Tollygunge premises of POSOCO. Balance 10%, deducted against Security Deposit, will be released 90 days after the end of contract period of three years subject to successful completion of contract and duly certified by the Executive-in -Charge.

3.3. Taxes & Duties

Work Contract Tax, Service tax, Income Tax etc. shall be deducted at source as applicable. All applicable taxes with rate as on date to be indicated in the bidding schedule.

3.4. Evaluation of Bid

The BID shall be evaluated on total price of the contract. Bids not covering the entire range of the scope of the contract shall not be considered for evaluation.

Technical Bid will be opened first. Bids with ambiguously filled Bid data sheet and/or Bids with which sufficient documentary proof supporting the Qualifying requirement and compliance of the product offered with TS is not available is liable for rejection.

Further, the Bidders will be called upon for face-to-face discussion of the technical details of the solution provided. Financial Bids of technically qualified bidders only will be opened after necessary intimation to the successful bidders.

Refer Note 2 of Bidding schedule (Section VI, Forms & Formats) Bids having Section A : Section B more than 65:35, i.e. bids received with cost of A greater than 65% of the total cost of contract is liable for rejection subject to modification of payment terms to accommodate such ratio.

3.5. Technical Qualification for participating in this Bid

Qualification of bidder will be based on meeting minimum pass /fail criteria specified below regarding the Bidder's or its collaborator's or its associates' technical experience and financial position as demonstrated by the Bidder's responses in the corresponding bid schedules. Technical experience and financial resources of any proposed sub-contractor shall not be taken in to account in determining the Bidder's compliance with the qualifying criteria.

Employer may assess the capacity and capability of the bidder, to successfully execute the scope of work covered under the package within stipulated completion period. The assessment shall inter-alia include:

(i) document verification

(ii) bidders work/manufacturing facilities visit

(iii) manufacturing capacity, details of work executed, works in hand, anticipated future & balance capacity available for the present scope of work

(iv) details of plant and machinery, manufacturing and testing facilities, manpower and financial resources

(v) details of quality systems in place

(vi) past experience and performance

(vii) customer feedback

(viii) Banker's feedback etc.

Employer reserves the right to waive minor deviations if they do not materially affect the capability of the bidder to perform the contract.

TECHNICAL EXPERIENCE

Authorized dealers and/or manufacturers and/or IT infrastructure solution providers having expertise in Hardware & Software supply & installation, Networking, Security implementation & services, IT Audit etc. with minimum 5 years of experience in the field of undertaking similar works for large Corporate/ Govt./ PSU or Private Organization fulfilling following minimum criteria are eligible viz.

i) The bidder or its collaborator must have supplied, installed, tested and commissioned at least One (1) installation in last 3 years of similar security system implementation project with the product of the same OEM as being offered against this NIT. Experience of executing SIEM service is preferable.

ii) The Network Monitoring & Security product offered should be NSS Lab recommended and is a globally recognized product in providing high-end Anti-APT detection & resolution platform. Necessary documentary proof in form of review, recommendations, certification & recognition should be submitted along with the offer.

iii) The AV suite offered should be in the Gartner Leaders Quadrant.

iv) The bidder or its collaborator has its own 24x7 support desk. The bidder must have at least 3 employees in its regular payroll having product specific certification from OEM / Recognized Institute for the product quoted. The bidder must have all required support / delivery engineers as mentioned in Para 4 of Section-V (TS) for Security management Service (in all 3 levels indicated) in his regular payroll on or before date of submission of the bid.

v) The bidder must submit tender specific authorization from the OEM for all the major products (Hardware / Software) supplied against the said NIT.

PREFERRABLE TECHNICAL EXPERTISE

The bidder or its collaborator preferably have minimum two (2) Cyber Security Expert & Forensic Analysis expert having suitable certification in implementation of IT Security Services & IT Security Audit such as ISSEP / CISSEP, SSCP, Cyber Security Forensic Analyst / CCFP, CCSP vaid for at least 1 year prior from date of publication of this NIT.

The bidder or its collaborator preferably have at least one certified Hardware professional having suitable certification on managing & installation of similar Anti-APT devices.

QUALITY ASSURANCE CERTIFICATION

The Bidder or its collaborator preferably have the following quality assurance certification issued by any authorized agency and valid as on the originally schedule date of bid opening.

Non-accreditation through above certification though does not disqualify the bidder for participation. However, necessary weightage for the same shall be given during technical evaluation.

a) ISO 9001:2008 Quality Management System

b) ISO 27001:2005 Information Security Management System (Preferable)

FINANCIAL POSITION

For the purpose of this particular bid, Bidders shall meet the following minimum criteria:

Minimum Average Annual Turnover*(MAAT) for the best two (2) years i.e 24 months out of last five (5) financial years of the bidder should minimum be Rs.2Crores.

Note: * Annual total income as incorporated in the Profit & Loss account except non recovery income e.g. sale of fixed assets.

In case bidder is a holding company, MAAT referred above shall be of that of holding company only (i.e. excluding its subsidiary /group companies). In case Bidder is a subsidiary of holding company, MAAT referred above shall be of that subsidiary company only (i.e. excluding its holding company).

Bidder must submit necessary documentary evidences in support of the pre-qualifying criteria stated above. Absence of sufficient documentary proof establishing bidders' compliance with the pre-qualifying requirements may lead to disqualification.

3.6. Other relevant details

1) The complete Bidding Documents including tender drawings (if, any) are available at ERLDC's website www.erldc.org and www.erldc.com Interested bidders can download the Bidding Documents and commence preparation of bids to gain time.

2) Interested eligible bidders may obtain further information from and inspect the Bidding Documents at the office of Chief Manager (C&M), ERLDC, POSOCO at the address given above from 10:00 hours (IST) to 17:00 hours (IST) on all working days during the period of sale of Bidding Documents.

3) **Tender Fees:** Interested Bidders will be required to furnish a nonrefundable fee of INR1250/- in the form of demand draft in favor of Power System Operation Corporation Ltd., payable at Kolkata on or before 17:00 hrs of 18.03.2016 .

4) The Bidding Documents are meant for the exclusive purpose of bidding against this specification and shall not be transferred to any other party or reproduced or used otherwise for any purpose other than for which they are specifically issued.

5) POSOCO reserves the right to cancel/withdraw this invitation for bids without assigning any reason and shall bear no liability whatsoever consequent upon such a decision.

6) All correspondence with regard to the above shall be to the following address (By Post/In Person).

A. Contractual Queries:

Chief Manager (C&M),
Eastern Regional Load Despatch Centre, Power System Operation Corporation Limited,
14, Golf Club Road, Tollygunge, Kolkata 700033
Telephone Nos.:- (Direct) +91-(0)33-24235014, Fax Nos.:- +91-(0)33-24235809

B. Technical Queries:

Senior Engineer (SL),
Eastern Regional Load Despatch Centre, Power System Operation Corporation Limited,
14, Golf Club Road, Tollygunge, Kolkata 700033
Telephone Nos.:- (Direct) +91-(0)33-30116933, Fax Nos.:- +91-(0)33-24235809

C. Financial Queries/Paying Authority:

Dy. General Manager (F&A),
Eastern Regional Load Despatch Centre, Power System Operation Corporation Limited,
14, Golf Club Road, Tollygunge, Kolkata 700033
Telephone Nos.:- (Direct) +91-(0)33-24235182, Fax Nos.:- +91-(0)33-24235809

For more information on ERLDC, POSOCO, visit our site at www.erldc.org or www.erldc.com

4. OTHER GENERAL CONDITIONS

4.1. Safety of Personnel

The bidder shall be responsible for the safety of your staff and workers while working in our premises against all accidents, damages or loss of life. It shall be your responsibility to immediately arrange for hospitalization, medical attendance in case of any accident or loss of life and it shall be your responsibility to meet the expenditure of such loss or accidents and to compensate for and/or arrange Insurance Coverage to your personnel. POSOCO, ERLDC shall not sustain any responsibility due to any damage suffered by your personnel on above grounds. However, you shall take utmost care towards safety of your personnel working in our premises.

4.2. Force Majeure

If this Contract during its continuance be prevented or delayed by reason of any War hostility, Acts of the public enemy, Civil commotion, National crisis, Sabotage, Fire, Flood, Earthquake, Lockout, Strike and any other Acts of God then provided notice of happening of such eventuality is given by the seller to the buyer within seven days from the date of its occurrence, neither party shall by reason of such eventuality be entitled to terminate the Contract and neither will the buyer have any claim for damage for delay in performance. However if the work is suspended by force majeure condition lasting more than two months, the purchaser shall have the option of canceling the Contract in whole or part thereof at his discretion.

4.3. Settlement of Disputes/Arbitration

All differences and/or disputes arising out of the contract shall be settled mutually but if required, the same would be resolved by arbitration as per the provision of the Arbitration & Conciliation Act 1996. G.M, ERLDC, POWER SYSTEM OPERATION CORPORATION LTD. shall be the sole arbitrator and if the G.M is unable or unwilling to act as the sole Arbitrator, some other person appointed by the Chairman & Managing Director, POWERGRID will be the Arbitrator. The award of the Arbitrator shall be final, conclusive and binding on all parties to the contract. The venue of the arbitration shall be such place as may be fixed by the Arbitrator. The cost of arbitration shall be borne by the parties to the dispute, as may be decided by the Arbitrator. The court of Kolkata shall have exclusive jurisdiction in all matters arising under the contract including execution of Arbitration awards.

4.4. Limitation of Liability

Notwithstanding anything contained herein, neither Party shall, in any event, regardless of the form of claim, be liable for any indirect, special, punitive, speculative, exemplary, consequential or incidental damages (including, without limitation, loss of use, data, revenue, profits, business), irrespective of whether it had an advance notice of the possibility of any such damages under this contract and the aggregate liability of the bidder, under this contract, shall not exceed the fees (excluding reimbursements) received by it under this contract during the six months preceding the date of such claim. Total Aggregate liability of the bidder for all claims shall not exceed the total fees received by them under this contract.

4.5. Information Security Assurance

The Bidder will be exposed, by virtue of the contracted activities, to internal business information of POSOCO, affiliates, business partners and /or customers. The bidder would be required to provide an undertaking that they will not use or pass to anybody the data/information derived by virtue of execution of this contract in any form. The bidder must safeguard the confidentiality of POSOCO, applications and data. For this bidder and his employees are required to sign Non-disclosure agreement with POSOCO.

Disclosure of any part of the afore mentioned information to parties not directly involved in providing the services requested, unless required to do so by the Court of Law or other Statutory Authorities, could result in premature termination of the contract. POSOCO may apart from blacklisting the bidder, initiate legal action against the bidder for breach of trust. The bidder shall also not make any news release, public announcements or any other reference on the development or contract without obtaining prior written consent from the POSOCO.

4.6. PF Certification Requirement

Certificate for statutory compliance to be submitted.

4.7. Compliance to SA 8000

The bidders are required to comply with the requirements of Social Accountability Standards (SA 8000:2008). The main clauses are enclosed (requirements of SA 8000:2008) along with the format for declaration regarding social accountability as Annexure. The enclosed declaration must be submitted along with the bid.

पावर सिस्टम ऑपरेशन कॉरपोरेशन लिमिटेड

POWER SYSTEM OPERATION CORPORATION LIMITED

पूर्वी क्षेत्रीय भार प्रेषण केन्द्र

Eastern Regional Load Despatch Centre

14 Golf Club Road, Tollygunge, Kolkata 700033

INSTRUCTION TO BIDDER (ITB)

For

IMPLEMENTATION OF MANAGED IT SYSTEM SECURITY SERVICE

And

NETWORK THREAT MONITORING, DETECTION AND RESOLUTION SERVICES

At ERLDC

SECTION - II

DOC Reference No. : ***ERLDC/C&M/1119/Antivirus etc/2016***	Issue Date: **February 25, 2016**

1. Title of the Project

Implementation of Managed IT System Security Service and Network Threat Monitoring, Detection & Resolution Services at ERLDC.

2. Preamble

This section (Section–II) of the Bidding Documents provides the information necessary for bidders to prepare responsive bids, in accordance with the requirements of the Employer. It also provides information on bid submission, opening and evaluation and on contract award. This Section (Section II) contains provisions that are to be used unchanged unless amended.

However, provisions governing the performance of the Contractor, payments under the contract or matters affecting the risks, rights and obligations of the parties under the contract are not included in this section but instead under Section – III: General Conditions of Contract and/or Section – IV: Special Conditions of Contract of this document.

Bidders may note that the Employer has uploaded its 'Works & Procurement Policy and Procedure' (Vol.-I & II) along with its Modification/Amendment on Capacity and Capability Assessment – regarding new parties undertaking to POWERGRID's website. Those Bidders who wish to peruse the same may visit www.powergridindia.com. However, it shall be noted that no other party, including the Bidder/Contractor, shall derive any right from this 'Works & Procurement Policy and Procedure' documents or have any claim on the Employer on the basis of the same. The respective rights of the Employer and Bidders/Contractors shall be governed by the Bidding Documents/Contracts signed between the Employer and the Contractor for the respective package(s). The provisions of Bidding Documents shall always prevail over that of 'Works & Procurement Policy and Procedure' documents in case of contradiction.

Further in all matters arising out of the provisions of this Section–II of the Bidding Documents, the laws of the Union of India shall be the governing laws and courts of Kolkata shall have exclusive jurisdiction.

3. The Owner/ Employer details:

Eastern Regional Load Despatch Centre, Power System Operation Corporation Limited
(A wholly owned subsidiary of POWERGRID)
14, Golf Club Road, Tollygunge, Kolkata 700033. INDIA
Telephone Nos.:- (Direct) +91-(0)33-24235867, Fax Nos.:- +91-(0)33-24235029

Kind Attn.: ***Contractual queries***: Chief Manager(C&M), ERLDC
Consignee: Chief Manager (SL), ERLDC
Paying Authority: Dy. General Manager (F&A), ERLDC

4. Introduction

4.1. Source of Funds

The Owner named above intends to use domestic funding (Owner's Internal Resources/Domestic Borrowings/Bonds) for this Project.

All eligible payments under the contract for the package for which this Invitation for Bids is issued shall be made by the designated paying authority of the owner named above in Indian Rupees.

4.2. Eligible Bidders

4.2.1 This Invitation for Bids, issued by the Employer is open to all firms including company(ies), Government owned Enterprises registered and incorporated in India as per Companies Act, 1956, and eligible to bid as per qualifying requirement described in cl.6.0 of IFB, barring Government Department as well as foreign bidders/MNCs not registered and incorporated in India and those bidders with whom business is banned by the Employer.

4.2.2 A Bidder shall not have a conflict of interest. All Bidders found to have a conflict of interest shall be disqualified. A Bidder may be considered to have a conflict of interest with one or more parties in this bidding process, if:

(a) they have a controlling partner in common; or

(b) they receive or have received any direct or indirect subsidy from any of them; or

(c) they have the same legal representative for purposes of this 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 Employer regarding this bidding process; or

(e) a Bidder submits more than one bid in this bidding process, either individually or as a partner in a joint venture, except for alternative offers permitted under clause 20..0. This will result in the disqualification of all such bids. However, this does not limit the participation of a Bidder as a subcontractor in another bid, or of a firm as a subcontractor in more than one bid; or

(f) a Bidder or any of its affiliates participated as a consultant in the preparation of the design or technical specifications of the Plant and Installation Services that are the subject of the bid.

(g) a Bidder or any of its affiliates has been hired (or is proposed to be hired) by the Employer as Project Manager for the contract.

4.2.3 The Bidder, directly or indirectly shall not be a dependent agency of the Employer.

4.3. Eligible Plant, Equipment and Services

4.3.1 For the purposes of these Bidding Documents, the words "facilities," "plant and equipment," "installation services," etc., shall be construed in accordance with the respective definitions given to them in the General Conditions of Contract.

4.3.2 All plant and equipment to be supplied and installed and services carried out under the contract shall have their origin in any country barring those countries against whom sanction for conducting businesses is imposed by Government of India and barring those firms with whom business is banned by the Employer.

4.3.3 For purposes of this clause, "origin" means the place where the plant and equipment or component parts thereof are mined, grown, or produced. Plant and equipment are produced when, through manufacturing, processing or substantial and major assembling of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

4.3.4 The origin of the plant, equipment, and services is distinct from the nationality of the Bidder.

4.4. Cost of Bidding

4.4.1 The Bidder shall bear all costs associated with the preparation and submission of its bid including post-bid discussions, technical and other presentations etc., and the Employer will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

5. The Bidding Document

5.1. Content of Bidding Documents

5.5.1 The facilities required, bidding procedures, contract terms and technical requirements are described in the Bidding Documents. The Bidding Documents comprise the following and shall include amendments, if any, thereto:

Section I	Invitation for Bids (IFB)
Section II	Instructions to Bidders (ITB)
Section III	General Conditions of Contract (GCC)
Section IV	Special Conditions of Contract (SCC)
Section V	Specifications and Scope of work
Section VI	Sample Forms and Format

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

5.2. Clarification of Bidding Documents;

5.2.1 A prospective Bidder requiring any clarification of the Bidding Documents may notify the Employer in writing or by cable (hereinafter, the term cable is deemed to include Electronic Data Interchange (EDI) or telefax) at the Employer's mailing address indicated in the BDS. Similarly, if a Bidder feels that any important provision in the documents, such as those listed in ITB Sub-Clause 19.3.1, will be unacceptable, such an issue should be raised as above. The Employer will respond in writing to any request for clarification or modification of the Bidding Documents that it receives no later than fourteen (14) days prior to the original deadline for submission of bids prescribed by the Employer. The Employer shall not be obliged to respond to any request for clarification received later than the above period. Further, the mere request for clarification from the Bidders shall not be a ground for seeking extension in the deadline for submission of bids. Written copies of the Employer's response (including an explanation of the query but not identification of its source) will be sent to all prospective bidders that have received the Bidding Documents.

5.2.2 The Bidder is advised to visit and examine the site(s) where the facilities are to be installed and its surroundings and obtain for itself on its own responsibility and cost all information that may be necessary for preparing the bid and entering into a contract for supply and installation of the facilities. The costs of visiting the site shall be at the Bidder's own expense.

5.2.3 The Bidder and any of its personnel or agents will be granted permission by the Employer to enter upon its premises and lands for the purpose of such inspection on prior request, but only upon the express condition that the Bidder, its personnel and agents will release and indemnify the Employer and its personnel and agents from and against all liability in respect thereof and will be responsible for death or personal injury, loss of or damage to property and any other loss, damage, costs and expenses incurred as a result of the inspection.

5.3. Amendment of Bidding Documents

5.3.1 At any time prior to the deadline for submission of bids, the Employer may, for any reason, whether at its own initiative, or in response to a clarification requested by a prospective Bidder, amend the Bidding Documents.

5.3.2 The amendment will be notified in writing or by cable to all prospective bidders who have purchased the Bidding Documents and will be binding on them. Bidders are required to immediately acknowledge receipt of any such amendment, and it will be assumed that the information contained therein will have been taken into account by the Bidder in its bid.

5.3.3 In order to afford reasonable time to the prospective Bidders to take the amendment into account in preparing their bid, the Employer may, at its discretion, extend the deadline for the submission of bids, in such cases, the Employer will notify all bidders in writing of the extended deadline.

6. Preparation of Bids

6.1. Language of Bid

6.1.1 The bid prepared by the Bidder and all correspondence and documents exchanged by the Bidder and the Employer related to the bid shall be written in the English language, provided that any printed literature furnished by the Bidder may be written in another language, as long as such literature is accompanied by English translation of its pertinent passages, in which case, for purposes of interpretation of the bid, the English translation shall govern.

6.2. Bid Currencies

6.2.1 Prices shall be quoted in Indian Rupees Only.

6.3. Bid Security

6.3.1 The Bidder shall furnish, as part of its bid, a bid security in the amount and currency as indicated below.

The amount of Bid Security shall be: Rs.46,800/- (Rupees Forty six thousand only)

6.3.2 The bid security shall, at the bidder's option, be in the form of a crossed bank draft/pay orders in favour of '**Power System Operation Corporation Limited**' payable at Kolkata from a reputed commercial bank or a bank guarantee from a scheduled commercial bank selected by the bidder and located in India. The format of the bank guarantee shall be in accordance with the form of bid security included in the Bidding Documents. Bid security shall remain valid for a period of thirty (30) days beyond the original bid validity period, and beyond any extension subsequently requested under ITB Sub-Clause 11.2.

6.3.3 Any bid not accompanied by a bid security or an acceptable bid security shall be rejected by the Employer as being non-responsive, pursuant to ITB Sub-Clause 19.4.

6.3.4 The bid securities of unsuccessful bidders will be returned as promptly as possible, but not later than twenty-eight (28) days after the expiration of the bid validity period.

6.3.5 The successful Bidder shall be required to keep its bid security valid for a sufficient period till the performance security(ies) pursuant to ITB Clause 31 are furnished to the satisfaction of the Employer. The bid security of the successful Bidder will be returned when the Bidder has signed the Contract Agreement, pursuant to ITB Clause 30, and has furnished the required performance security, pursuant to ITB Clause 35.

6.3.6 The bid security may be forfeited

(a) if the Bidder withdraws its bid during the period of bid validity specified by the Bidder in the Bid Form; or

(b) In case the Bidder does not withdraw the deviations proposed by him, if any, at the cost of withdrawal stated by him in the bid; or

(c) If a Bidder does not accept the corrections to arithmetical errors identified during preliminary evaluation of his bid pursuant to ITB Sub-Clause 24.2; or

(d) in the case of a successful Bidder, if the Bidder fails within the specified time limit

(i) to sign the Contract Agreement, in accordance with ITB Clause 30, or

(ii) to furnish the required performance security(ies), in accordance with ITB Clause 31 and/or to keep the bid security valid as per the requirement of ITB Sub-Clause 10.5.

6.3.7 No interest shall be payable by the Employer on the above Bid Security.

6.4. Period of Validity of Bid

6.4.1 Bids shall remain valid for the period of six months after the date of opening of Techno - Commercial Part i.e. First Envelope, prescribed by the Employer, pursuant to ITB Sub-Clause 17.1. A bid valid for a shorter period shall be rejected by the Employer as being non-responsive.

6.4.2 In exceptional circumstance, the Employer may solicit the Bidder's consent to an extension of the bid validity period. The request and responses thereto shall be made in writing or by cable. If a Bidder accepts to prolong the period of validity, the bid security shall also be suitably extended. A Bidder may refuse the request without forfeiting its bid security. A Bidder granting the request will not be required or permitted to modify its bid.

6.5. Format and Signing of Bid

6.5.1 The bid shall contain no alterations, omissions or additions, unless such corrections are initialed by the person or persons signing the bid.

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

7. Submission of Bids

7.1. Submission of Bids

7.1.1 The Bidder shall submit the bid on line in two part i.e First Part (Techno – Commercial Part) and Second Part (Price Part).

First Part (Technical Part) Bid consisting inside the following

a) Integrity Pact (in original)

b) Bid Security (in original)

c) Techno-Commercial Offer.(on line)

Second Part (Price Part):

Price Bid".

7.1.2 **Bid Securities and the Integrity Pact** in original shall be submitted in separate superscripted envelopes (one for Bid Security and another for Integrity Pact) within the stipulated date.

All the envelopes shall also indicate the name and address of the Bidder so that the bid can be returned unopened in case it is declared "late."

7.1.3 If the envelope is not sealed and marked as required by ITB Sub-Clause 7.1.2 above, the Employer will assume no responsibility for the bid's misplacement or premature opening. If the outer envelope discloses the Bidder's identity, the Employer will not guarantee the anonymity of the bid submission, but this disclosure will not constitute grounds for bid rejection.

7.2. Deadline for Submission of Bids

7.2.1 Bids must be submitted by the bidder no later than the time and date specified. In the event of the specified date for the submission of bids being declared a holiday for the Employer, the bids will be received up to the appointed time on the next working day. Bids once submitted by the bidder shall not be returned except otherwise provided in the Bidding Documents.

Last Date & Time of submission of BID: 17:00 Hrs. 21.03.2016.

7.2.2 The Employer may, at its discretion, extend this deadline for submission of bids by amending the Bidding Documents in accordance with ITB Sub-Clause 7.3 for the reasons specified therein at any time prior to opening of bids by the Employer pursuant to ITB Clause 20, in which case all rights and obligations of Employer and bidders will thereafter be subject to the deadline as extended.

15. Late Bids

15.1 Any bid received by the Employer after the bid submission deadline prescribed by the Employer, pursuant to ITB Clause 14, will be rejected and returned unopened to the Bidder.

16. Modification and Withdrawal of Bids

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

16.2 The Bidder's modifications shall be prepared, sealed, marked and dispatched as follows:

(a) The Bidders shall provide an original and two number of copies of any modifications to its bid, clearly identified as such, in two inner envelopes duly marked "Bid Modifications …… Envelope —Original" and "Bid Modifications …… Envelope —Copies." The inner envelopes shall be sealed in an outer envelope, which shall be duly marked "Bid Modifications."

(b) Other provisions concerning the marking and dispatch of bid modifications shall be in accordance with ITB Sub-Clauses 13.2, 13.3 and 13.4.

16.3 A Bidder wishing to withdraw its bid shall notify the Employer in writing prior to the deadline prescribed for bid submission. The notice of withdrawal shall

(a) be addressed to the Employer at the address named owner / employer details, and

(b) bear the contract name, the IFB number, and the words "***Bid Withdrawal Notice***." Bid withdrawal notices received after the bid submission deadline will be ignored, and the submitted bid will be deemed to be a validly submitted bid.

16.4 No bid may be withdrawn in the interval between the bid submission deadline and the expiration of the bid validity period specified in ITB Clause 11. Withdrawal of a bid during this interval may result in the Bidder's forfeiture of its bid security, pursuant to ITB Sub-Clause 10.6.

E. Bid Opening and Evaluation

17. Opening of First Part by Employer

17.1 The Employer will open the First Part i.e. Technical Part on line, including withdrawals and modifications made pursuant to ITB Clause 16, in the presence of bidders' designated representatives who choose to attend, at the time, date, and location stipulated below.

Date & Time of Opening of First part: 15:00 Hrs. 22.03.2016.

The bidders' representatives who are present shall sign a register evidencing their attendance. In the event of the specified date for the submission of bids being declared a holiday for the Employer, the bids will be received up to the appointed time on the next working day.

17.2 For all the Bids, the bidders' names, the presence of bid security, Integrity Pact and any such other details as the Employer may consider appropriate, will be announced by the Employer at the opening. Subsequently, all documents marked "Modification" shall be opened and the submissions therein read out in appropriate detail. No bid shall be rejected at bid opening except for late bids pursuant to ITB Clause 15 and bid not accompanied by a duly signed Integrity Pact and bid security. Such bids shall not be entertained. However, opening of bid, whether or not accompanied with the bid security, shall not be construed to imply its acceptability which shall be examined in detail pursuant to the provisions contained in this Section-II.

On behalf of Employer, the Integrity Pact will be signed by its representative at the time of Bid Opening. One original of the Integrity Pact will be retained by Employer and the other original will be returned to the representative of the bidders present during bid opening. If the Bidder's representative is not present during the Bid Opening, the other original shall be sent to the bidder by post/courier.

17.4 The Employer shall prepare minutes of the bid opening in the form of Bid Opening Statement, including the information disclosed to those present in accordance with ITB Sub-Clause 17.3.

17.5 Bids not opened at bid opening shall not be considered further for evaluation, irrespective of the circumstances and shall be returned to the Bidder unopened.

18. Clarification of Bids

18.1 During bid evaluation, the Employer may, at its discretion, ask the Bidder for a clarification of its bid. The request for clarification and the response shall be in writing, and no change in the price or substance of the bid shall be sought, offered or permitted.

19. Preliminary Examination of Technical part (Part-I)

19.1 The Employer will examine the bids to determine whether they are complete, whether required sureties have been furnished, whether the documents have been properly signed, and whether the bids are generally in order.

19.2 The Employer may waive any minor informality, nonconformity or irregularity in a bid that does not constitute a material deviation, whether or not identified by the Bidder.

19.3 Prior to the detailed evaluation, the Employer will determine whether each bid is of acceptable quality, is complete and is substantially responsive to the Bidding Documents. Any deviations, conditionality or reservation introduced in the Bid Form, Technical Data Sheets and covering letter, or in any other part of the bid will be reviewed to conduct a determination of the

substantial responsiveness of the bidder's bid. For purposes of this determination, a substantially responsive bid is one that conforms to all the terms, conditions and specifications of the Bidding Documents without material deviations, objections, conditionalities or reservations. A material deviation, objection, conditionality or reservation is one (i) that affects in any substantial way the scope, quality or performance of the contract; (ii) that limits in any substantial way, inconsistent with the Bidding Documents, the Employer's rights or the successful Bidder's obligations under the contract; or (iii) whose rectification would unfairly affect the competitive position of other bidders who are presenting substantially responsive bids.

19.3.1 Bids containing deviations from critical provisions relating to GCC Clauses 8.0 (Governing Law), 9.1 (Terms of Payment), 6.0 (Performance Security), 18 (Taxes and duties, 21.0 (Limitation of Liability), 22.0 (Settlement of Disputes), 16.0 (Arbitration) and Form of Contract Agreement (Price Adjustment) will be considered as non-responsive.

19.3.2 Regarding deviations, conditionality or reservations introduced in the bid, which will be reviewed to conduct a determination of substantial responsiveness of the Bidder's bid as stated in ITB Sub-Clause 19.3, the order of precedence of these documents to address contradictions, if any, in the contents of the bid, shall be as follows:

I. Covering Letter

II. Bid Form

III. Technical Data Sheet

IV. Any other part of the bid

Contents of the document at Sr. No. I above will have overriding precedence over other documents (Sr. No. II to IV above).Similarly, contents of document at Sr. No. II above will have overriding precedence over other documents (Sr. No. III to IV above), and so on.

19.4 If a bid is not substantially responsive, it will be rejected by the Employer, and may not subsequently be made responsive by the Bidder by correction of the nonconformity. The Employer's determination of a bid's responsiveness is to be based on the contents of the bid itself without recourse to extrinsic evidence.

20. Qualification

20.1 The Employer will ascertain to its satisfaction whether Bidders determined having submitted substantially responsive bids are qualified, as per the Qualification Requirement specified in cl.6.0 of IFB to satisfactorily perform the contract. The Employer shall be the sole judge in this

regard and the Employer's interpretation of the Qualification Requirement shall be final and binding.

20.2 The determination will take into account the Bidder's financial, technical capabilities including production capabilities, in particular the Bidder's contract work in hand, future commitments & current litigation and past performance. It will be based upon an examination of the documentary evidence of the Bidder's qualifications submitted by the Bidder to the bid, as well as such other information as the Employer deems necessary and appropriate. This shall, however, be subject to assessment that may be carried out, if required, by the Employer as per the provisions of cl.6.0 of IFB. The employer shall be the sole judge in this regard.

20.3 Each Bidder shall submit with its Techno- Commercial Part (First Part) the following attachments:

(a) Attachment 1: Bid Security

A bid security in sealed separate envelope shall be furnished in accordance with ITB Clause 10 & ITB Clause 13.

(b) Attachment 2: Integrity Pact

The Bidder shall complete the accompanying Integrity Pact, which shall be applicable for bidding as well as contract execution, duly signed on each page by the person signing the bid and shall be returned by the Bidder in two (2) originals along with the Techno - Commercial Part in a separate envelope, duly superscripted with 'Integrity Pact'. The Bidder shall submit the Integrity Pact on a non-judicial stamp paper of Rs.100/-. If the Bidder is a partnership firm or a consortium, the Integrity Pact shall be signed by all the partners or consortium members. Bidder's failure to submit the Integrity Pact duly signed along with the Bid shall lead to outright rejection of the Bid.

(c) Attachment 3: Power of Attorney

A power of attorney, duly notarized, indicating that the person(s) signing the bid has(ve) the authority to sign the bid and thus that the bid is binding upon the Bidder during full period of its validity, in accordance with ITB Clause 11.

(d) Attachment 4: Bidder's Eligibility and Qualifications

In the absence of prequalification, documentary evidence establishing that the Bidder is eligible to bid in accordance with ITB Clause 2 and is qualified to perform the contract in accordance with qualifying requirement described in cl.6.0 of IFB, if its bid is accepted.

The documentary evidence of the Bidder's eligibility to bid shall establish to the Employer's satisfaction that the Bidder, at the time of submission of its bid, is eligible as defined in ITB Clause 2.

The documentary evidence of the Bidder's qualifications to perform the contract, if its bid is accepted, shall establish to the Employer's satisfaction that the Bidder has the financial, technical, production, procurement, shipping, installation and other capabilities necessary to perform the contract, and, in particular, meets the experience and other criteria outlined in the Qualifying Requirement of the Bidder described in cl.6.0 of IFB and shall also include:

The complete annual reports together with Audited statement of accounts of the company for last five years of its own (separate) immediately preceding the date of submission of bid.

[**Note I**. In the event the Bidder is not able to furnish the above information of its own (i.e., separate), being a subsidiary company and its accounts are being consolidated with its Group/ Holding/ Parent company, the Bidder should submit the audited balance sheet, income statement, other information pertaining to it only (not of its Group/Holding/Parent company) duly certified by any one of the authority [(i) Statutory Auditor of the Bidder/(ii) Company Secretary of the Bidder a (iii) A certified Public Accountant] certifying that such information/documents are based on the audited accounts as the case may be.]

[**Note II**. Similarly, if the Bidder happens to be a Group/Holding/ Parent company, the Bidder should submit the above documents/information of its own (i.e., exclusive of its subsidiaries) duly certified by any one of the authority mentioned in Note I above certifying that these information/documents are based on audited accounts, as the case may be.]

Unless otherwise mentioned in the Bid document, bids submitted by a joint venture/authorized service provider of original air conditioning manufacturer, if allowed as per stipulated Qualifying Requirement of the Bidder described in cl.6.0 of IFB, shall comply with the following requirements:

(i) The bid shall include all the information required for Attachment 3 as described above for each joint venture /authorized service provider of original air conditioning manufacturer.

(ii) The bid shall be signed so as to be legally binding on all partners.

(iii) Joint venture/authorized service provider of original air conditioning manufacturer shall be liable jointly and severally for the execution of the contract in accordance with the contract terms.

(vi) A copy of the agreement entered into by the joint venture partners shall be submitted with the bid as per Form-6 of Section -IV, including interalia delineation of

responsibilities and obligations of each partners appended thereto, notwithstanding the joint and several liability.

In order for a joint venture/authorized service provider of original air conditioning manufacturer to qualify, each of its partners or combination of partners must meet the minimum criteria listed in the Qualifying Requirement of the Bidder described in cl.6.0 of IFB for an individual Bidder for the component of the contract they are designated to perform. Failure to comply with this requirement will result in rejection of the joint venture /authorized service provider of original air conditioning manufacturer bid.

A firm can be a partner in only one joint venture/authorized service provider of original air conditioning manufacturer; bids submitted by joint ventures or consortia including the same firm as partner will be rejected.

(e) Attachment 5: Declaration regarding Social Accountability

The Bidder shall complete the accompanying **Declaration regarding Social Accountability (sa-8000) as per section –VI of this NIT (FORMS AND FORMATS)**, duly signed by the person signing the bid and shall be returned by the Bidder.

(f) Attachment 7: Information for E-payment, PF details Including statutory declaration for PF in prescribed format and declaration regarding Micro/Small & Medium Enterprises

(g) Attachment 8: Additional Information

(i) Certificate from their Banker(s) indicating various fund based/non fund based limits sanctioned to the Bidder and the extent of utilization as on date. Such certificate should have been issued not earlier than three months prior to the date of bid opening. Wherever necessary the Employer may make queries with the Bidders' Bankers.

(ii) Detailed information on any litigation or arbitration arising out of contracts completed or under execution by it over the last five years. A consistent history of awards involving litigation against the Bidder or any partner of JV may result in rejection of Bid.

(iii) Any other information which the Bidder intends to furnish.

(h) Attachment 9: Bidding schedule.

20.4 The Employer may waive any minor informality, nonconformity or irregularity in a bid that does not constitute a material deviation, affecting the capability of the Bidder to perform the Contract.

20.5 An affirmative determination will be a prerequisite for the Employer to evaluate the Techno - Commercial Part and open the Second Envelope of the Bidder. A negative determination will result in rejection of the Bidder's bid.

21. Evaluation of Techno - Commercial Part (First Envelope)

21.1 The Employer will carry out a detailed evaluation of the bids of the qualified bidders in order to determine whether the technical aspects are in accordance with the requirements set forth in the Bidding Documents. In order to reach such a determination, the Employer will examine the information supplied by the bidders, and other requirements in the Bidding Documents, taking into account the following factors:

(a) overall completeness and compliance with the Technical Specifications; suitability of the facilities offered in relation to the environmental and climatic conditions prevailing at the site; and quality, function and operation of any process control concept included in the bid. The bid that does not meet minimum acceptable standards of completeness, consistency and detail will be rejected for non-responsiveness.

(b) achievement of specified performance criteria by the facilities

(c) acceptance of AMC terms & conditions by the bidder with time schedule, spares, manpower availability etc. during AMC period as indicated in the bidding document.

(d) type, quantity and long-term availability of mandatory and recommended spare parts and maintenance services

(e) any other relevant technical factors that the Employer deems necessary or prudent to take into consideration.

(f) any deviations to the commercial and contractual provisions stipulated in the Bidding Documents.

22. Opening of Price part (Part-II) :

22.1 The Second Envelope i.e., Price Part of only those Bidders shall be opened who are determined as having submitted substantially responsive bids and are ascertained to be qualified to satisfactorily perform the Contract, pursuant to ITB Clause 20 and 21. Such Bidders shall be intimated about the date and time for opening of Price Part i.e., Second Envelope of the Bids by the Employer. A negative determination of the bids pursuant to ITB Clause 20 and 21, shall be notified by the Employer to such Bidders and the Second Envelope submitted by them shall not be opened and bid security shall be returned.

22.2 The Employer will open **Second Part i.e., Price Part** at the specified time and date in the presence of bidders' designated representatives who choose to attend, at the time, date, and location stipulated in the intimation for opening of Second Envelope. The bidders' representatives who are present shall sign a register evidencing their attendance.

22.3 The bidders' names, the Bid Prices, including any alternative Bid Price or any discounts, and any such other details as the Employer may consider appropriate, will be announced by the Employer at the opening. The prices and details as may be read out during the bid opening and recorded in the Bid Opening Statement would not be construed to determine the relative ranking amongst the Bidders, or the successful Bidder, and would not confer any right or claim whatsoever on any Bidder. The successful Bidder (also referred to as the L1 Bidder) shall be determined as per the provisions of this Section – II and considered for award of contract as provided in ITB Clause 27.

22.4 The Employer shall prepare minutes of the bid opening, including the information disclosed to those present in accordance with ITB Sub-Clause 22.3.

22.5 Bids not opened and read out at bid opening shall not be considered further for evaluation, irrespective of the circumstances.

23. Conversion to Single Currency

23.1 This shall not be applicable as domestic firms are required to quote the prices in Indian Rupees only.

24. Evaluation of Second Part (Price Part)

24.1 The Employer will examine the Price Parts (Second Envelopes) to determine whether they are complete, whether any computational errors have been made, whether the documents have been properly signed, and whether the bids are generally in order.

The Price Part containing any deviations and omissions from the contractual and commercial conditions and the Technical Specifications which have not been identified in the First Envelope are liable to be rejected.

24.2 Arithmetical errors will be rectified on the following basis. If there is a discrepancy between the unit price and the total price, which is obtained by multiplying the unit price and quantity, or between subtotals and the total price, the unit or subtotal price shall prevail, and the total price shall be corrected. However, in case of items quoted without indicating any quantity or the items for which the quantities are to be estimated by the Bidder, the total price quoted against such items shall prevail. If there is a discrepancy between words and figures, the amount in words will prevail. The subtotal, total price or the total bid price, irrespective of the discrepancy

between the amount indicated in words or figures shall be rectified in line with the procedure explained above. If the Bidder does not accept the correction of errors, its bid will be rejected and the amount of Bid Security forfeited.

The prices of all such item(s) against which the Bidder has not quoted rates/amount (viz., items left blank or against which '-' is indicated) in the Price Schedules will be deemed to have been included in other item(s).

If the discount(s)/rebate(s) offered by the Bidder is a percentage discount and the price component(s) on which the said discount is not indicated in the bid, the same shall be considered on the total bid price [i.e. proportionately on each price component], in the event of award. However, if lump-sum discount is offered, the same shall be considered in full on the Ex-works price component (by proportionately reducing Ex-works price of individual items), in case of award. Further, Conditional discounts/rebates, if any, offered by the bidder shall not be taken into consideration for evaluation. It shall, however, be considered in case of award.

In respect of taxes, duties and other levies indicated by the Bidder in the Bid, which are reimbursable in line with the provisions of the Bidding Documents, the applicable rate and amount thereof shall be ascertained by the Employer based on which, if required, necessary rectification and arithmetical correction shall be carried out by the Employer. The rate and amount so ascertained by the Employer shall prevail.

The Bidder should ensure that the prices furnished in various price schedules are consistent with each other. In case of any inconsistency in the prices furnished in the specified price schedules to be identified in Bid Form for this purpose, the Employer shall be entitled to consider the highest price for the purpose of evaluation and for the purpose of award of the Contract use the lowest of the prices in these schedules.

24.3 The comparison shall be on the total price. No individual price comparison shall be made.

The comparison shall also include the applicable taxes, duties and other levies, which are reimbursable in line with the provisions of the Bidding Documents.

24.4 Any adjustments in price that result from the above procedures shall be added, for purposes of comparative evaluation only, to arrive at an "Evaluated Bid Price." Bid prices quoted by bidders and rectified as per ITB Sub Clause 24.2 shall remain unaltered.

25. Purchase/ Domestic Preference

25.1 Purchase Preference as admissible under the policy of Government of India in vogue will be allowed to Central Public Sector Enterprises in evaluation and comparison of bids.

26. *Confidentiality and Contacting the Employer*

26.1 After the public opening of bids, information relating to the examination, clarification, and evaluation of bids and recommendations concerning awards shall not be disclosed to Bidders or other persons not officially concerned with this process until the publication of contract award. From the time of bid opening to the time of contract award, if any Bidder wishes to contact the Employer on any matter related to its bid, it should do so in writing.

26.2 Any effort by a Bidder to influence the Employer in the Employer's bid evaluation, bid comparison or contract award decisions may result in rejection of the Bidder's bid. The Employer shall be the sole judge in this regard.

F. Award of Contract

27. *Award Criteria*

27.1 Subject to ITB Clause 28, the Employer will award the contract to the successful Bidder (also referred to as the L1 Bidder) whose bid has been determined to be substantially responsive and to be the lowest evaluated bid, further provided that the Bidder is determined to be qualified, as per the Qualification Requirement specified in cl.6.0 of IFB to perform the contract satisfactorily.

27.2 The Employer may request the Bidder to withdraw any of the deviations listed in the winning bid.

28. *Employer's Right to Accept any Bid and to Reject any or all Bids*

28.1 The Employer reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected Bidder or bidders or any obligation to inform the affected Bidder or bidders of the grounds for the Employer's action.

29. *Notification of Award*

29.1 Prior to the expiration of the period of bid validity, the Employer will notify the successful Bidder in writing, that its bid has been accepted. The notification of award will constitute the formation of the contract.

29.2 The Employer shall publish the results on its website, identifying the bid and Specification numbers and the following information: (i) name of each Bidder who submitted a Bid; (ii) bid prices as read out at bid opening; (iii) name and evaluated prices of each Bid that was evaluated; (iv) name of bidders whose bids were rejected and the reasons for their rejection; and (v) name

of the winning Bidder, and the price it offered, as well as the duration and summary scope of the contract awarded.

The Employer shall promptly respond in writing to any unsuccessful Bidder who, after notification of award in accordance with above, requests in writing the grounds on which its bid was not selected.

29.3 Upon the successful Bidder's furnishing of the performance security pursuant to ITB Clause 31, the Employer will promptly discharge the bid securities, pursuant to ITB Sub-Clause 10.4 & 10.5.

30. Signing the Contract Agreement

30.1 At the same time as the Employer notifies the successful Bidder that its bid has been accepted, the Employer in consultation with the Bidder will prepare the Contract Agreement provided in the Bidding Documents, incorporating all agreements between the parties.

30.2 The Contract Agreement shall be prepared within twenty-eight (28) days of the Notification of Award and the successful Bidder and the Employer shall sign and date the Contract Agreement immediately thereafter.

31. Performance Security

31.1 Within twenty-eight (28) days after receipt of the Notification of Award, the successful Bidder shall furnish the performance security for 10% (Ten percent) of the contract price plus additional performance securities, if any, in line with the requirement of this bidding document.

31.2 Security Deposit:-10% of the Billed amount of the successful bidder shall be deducted towards security deposit from all running/final bills towards faithful performance of contract. The amount so deducted shall be released 90 days after the end of contract period of two years subject to successful completion of contract and duly certified by the Engineer-in-Charge. The EMD submitted along with the Bid shall be released after deduction of security deposit.

31.2 Failure of the successful Bidder to comply with the requirements of ITB Clause 30 or Clause 31 shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security.

32. Payment Terms

100% of the billed amount of the successful bidder, who opted for CPG shall be released within 15 days by e- payment after successful implementation of the job as certified by the Engineer-

in -charge or by the CONSIGNEE at the Tollygunge premises of POSOCO. The payment will be released subject to submission of valid CPG.

Alternatively

90% of monthly billed amount shall be released within 15 days by e-payment after successful implementation of the job as certified by the Engineer- in -charge or by the CONSIGNEE at the Tollygunge premises of POSOCO. Balance 10%, deducted against Security Deposit, will be released 90 days after the end of contract period of three years subject to successful completion of contract and duly certified by the Executive-in -Charge

33. Fraud and Corruption

It is the Employer's policy that requires the Bidders, suppliers and contractors and their subcontractors under the contracts to 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 purpose of this provision, the terms set forth below as follows:

(i) "corrupt practice" is the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party;

(ii) "fraudulent practice" is any act or omission, including a misrepresentation, that knowingly or recklessly misleads or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation;

(iii) "collusive practice" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party;

(iv) "coercive practice" is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party;

(v) "obstructive practice" is

(aa) deliberately destroying, falsifying, altering or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede an Employer's investigation into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation;

Or (bb) acts intended to materially impede the exercise of the Employer's inspection and audit rights.

(b) will reject a proposal for award if it determines that the bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive, coercive or obstructive practices in competing for the contract in question;

(c) will sanction a firm or individual, including declaring ineligible, either indefinitely or for a stated period of time, to be awarded a contract if it at any time determines that the firm has, directly or through an agent, engaged in corrupt, fraudulent, collusive, coercive or obstructive practices in competing for, or in executing, a contract; and

(d) will have the right to require that the provision be included in Bidding Documents and in contracts, requiring Bidders, suppliers, and contractors and their sub-contractors to permit the Employer to inspect their accounts and records and other documents relating to bid submission and contract performance and to have them audited by auditors appointed by the Employer.

----- End of Section-II (ITB) ----

POWER SYSTEM OPERATION CORPORATION LIMITED

Eastern Regional Load Despatch Centre

14 Golf Club Road, Tollygunge, Kolkata 700033

SECTION - III

GENERAL CONDITION OF CONTRACT

For

IMPLEMENTATION OF MANAGED IT SYSTEM SECURITY SERVICE

And

NETWORK THREAT MONITORING, DETECTION AND RESOLUTION SERVICES

At ERLDC

(E-TENDERING)

DOC Reference No. : ***ERLDC/C&M/1119/Antivirus etc/2016***	Issue Date: **February 26, 2016**

A. TITLE OF THE PROJECT

Implementation of Managed IT System Security Service and Network Threat Monitoring, Detection & Resolution Services at ERLDC.

B. DEFINITIONS

1.0 **Definitions and Interpretation**

1.1 **Definitions**

In the Contract (as hereinafter defined) the following words and expressions shall have the meanings hereby assigned to them:

1.1.1 "Commencement Date" means the date of Notification of Award (NOA)/Letter of Award (LOA) or any other date specified therein.

1.1.2 "Conditions" means these General Conditions of Contract, and the Special Conditions of Contract.

1.1.3 "Contract" means the agreement between the Purchaser and the Supplier for the execution of the works incorporating the Conditions, Specification, price & other completed Schedules, Bid, Notification of Award/ Letter of Award and such further documents as may be expressly incorporated in the Notification of Award/ Letter of Award.

1.1.4 "Contract Agreement" means the document recording the terms of the Contract between the Purchaser and the Supplier.

1.1.5 "Contract Price" means the sum stated in the Notification of Award/ Letter of Award as payable to the Supplier for execution and commissioning of the works and adjusted, after optimization, on the basis provided in the Contract. It shall be the sum total of all the amounts entered by the Supplier in the Schedule of Prices.

1.1.6 "Supplier" means the person whose Bid has been accepted by the Purchaser and the legal successors in title to the Supplier but not (except with the consent of the Purchaser) any assignee of the Supplier.

1.1.7 "Force Majeure" has the meaning assigned to it under Sub-clause 11.0.

1.1.8 "Foreign Currency" means a currency of a country other than that in India.

1.1.9 "Notification of Award/Letter of Award" means the formal award by the Purchaser of the Bid incorporating any adjustments or variations to the Bid agreed between the Purchaser and the Supplier.

1.1.10 "Performance Security" means the security to be provided by the Supplier in accordance with Sub-clause 6.1 for the due performance of the Contract.

1.1.11 "Purchaser" or "Owner" means Power System Operation Corporation Ltd., ERLDC, Kolkata and the legal successors in title to the Purchaser but not (except with the consent of the Supplier) any assignee of the Purchaser.

1.1.12 "Site" means the place or places, where work is to be done by the Supplier.

1.1.13 "Bid" means the Supplier's priced offer to the Purchaser for the execution of the Works.

1.1.14 "Works" means all services to be supplied and services to be provided by the Supplier under the Contract.

1.1.15 "Government" means the Government of India.

1.1.16 The word "Supplier" wherever appears shall carry the same meaning as that of Contractor/Bidder.

1.1.17 "Plant and Equipment" means permanent plant, equipment, machinery, apparatus, articles and things of all kinds to be provided and incorporated in the Facilities by the Contractor under the Contract (including the spare parts to be supplied by the Contractor under GCC Sub-Clause 3.3 hereof), but does not include Contractor's Equipment.

1.2 **Headings and Titles**

The headings and titles in these Conditions shall not be deemed part thereof or be taken into consideration in the interpretation or construction of the Contract.

1.3 **Written Communications**

Wherever in the Contract provision is made for a communication to be "written" or "in writing" this means any hand-written, type written or printed communication including facsimile transmission.

C. TERMS & CONDITIONS

2.0 **Engineer-in-Charge**

2.1 The Purchaser shall appoint an experienced senior engineer responsible to the Purchaser and designated as the Engineer-in-Charge who shall carry out the functions and obligations of the Purchaser under the Contract exercising such authority as delegated to him.

2.2 The Contractor shall appoint an experienced senior engineer responsible to the Contractor and designated as the Engineer-in-Charge who shall carry out the functions and obligations of the Contractor under the Contract exercising such authority as delegated to him.

3.0 **Assignment**

The Supplier shall not assign the Contract or any part of his obligations under the Contract without the prior written consent of the Purchaser (which shall not be unreasonably withheld). A charge in favour of the Supplier's bankers of any monies due under the Contract shall not be considered an assignment.

4.0 **Contract Documents**

4.1 **Ruling Language**

Where versions of the Contract are prepared in different languages the English version shall prevail.

4.2 **Day-to-Day Communications**

The day-to-day communications shall be in English language only.

4.3 **Priority of Contract Documents**

Unless otherwise provided in the Contract the order of priority of-the Contract documents shall be as follows (SI. No. 1 being the top priority):

1. The Notification of Award/ Letter of Award

2. The Special Conditions of Contract
3. The System Required Specifications
4. The General Conditions of Contract
5. Any other documents forming part of the Contract.

5.0 **Contract Agreement**

5.1 The Supplier shall execute a Contract Agreement recording all the terms of the Contract, to be prepared by and completed at the cost of the Supplier.

6.0 **Performance Security**

6.1 The Supplier shall obtain a Performance Security, in the sum of 10% of the total Contract Price within 28 days of issuance of the Notification of Award/ Letter of Award. The Performance Security shall be provided by a person and in a form approved by the Purchaser. The cost of complying with the requirements of this Clause shall be borne by the Supplier. The security shall be furnished valid initially till three months after the expiry of the contract period and shall be extended appropriately as contract period is extended.

The form of the Performance Security shall be as provided in Section-VI FORMS of the Bidding Documents. In the event of any change in the Contract Price, the Performance Security shall be adjusted provided that such adjustment shall be subject to the approval of the Purchaser. The Performance Security shall be paid to the Purchaser on first demand without conditions or proof.

The Performance Security for the Works shall be in a freely convertible currency acceptable to the Purchaser or in US dollars.

6.2 **Period of Validity**

The Performance Security shall be valid until the Supplier has executed and completed the Works in accordance with the Contract. No claim shall be made against the Performance Security after the completion of contract and the Performance Security shall be returned to the Supplier at the earliest as per the contract.

7.0 **Contract Price**

7.1 Sufficiency of Contract Price.

The Contractor shall be deemed to have satisfied himself of and taken account of in his Bid:

a) All conditions and circumstances affecting the Contract Price,

b) Physical location & access to various sites.

If the specification does not contain particulars of activities which are obviously necessary for proper completion of the service to system/works and the intention to include which is nevertheless to be inferred, all such activities shall be executed by the Supplier without extra charge. If the Supplier requires additional information, he shall so request in writing to the Purchaser, who will provide such detailed information as necessary within a reasonable time.

8.0 **Compliance with Laws**

8.1 The Supplier shall comply with the laws of the country of works and the laws of India where the same is to be carried out.

9.0 **Certificates and Payment**

9.1 **Terms of Payment**

100% of the billed amount of the successful bidder, who opted for CPG shall be released within 15 days by e- payment after successful implementation of the job as certified by the Engineer-in -charge or by the CONSIGNEE at the Tollygunge premises of POSOCO. The payment will be released subject to submission of valid CPG.

Alternatively

90% of monthly billed amount shall be released within 15 days by e-payment after successful implementation of the job as certified by the Engineer- in -charge or by the CONSIGNEE at the Tollygunge premises of POSOCO. Balance 10%, deducted against Security Deposit, will be released 90 days after the end of contract period of three years subject to successful completion of contract and duly certified by the Executive-in -Charge.

10.0 **Foreign Currency**

10.1 **Payment in Foreign Currencies**

Payment in foreign currencies shall be made in accordance with the Schedule of Prices submitted by the Supplier with his Bid and incorporated in the Notification of Award/ Letter of Award.

11.0 **Force Majeure**

11.1 **Definition of Force Majeure**

Force Majeure means any circumstances beyond the control of the parties, including but not limited to:

a) war and other hostilities, (whether war be declared or not), invasion, act of foreign enemies, mobilisation, requisition or embargo;

c) ionising radiation or contamination by radioactivity from any nuclear fuel or from any nuclear waste from the combustion of nuclear fuel, radioactive toxic explosives, or other hazardous properties of any explosive nuclear assembly or nuclear components thereof;

d) rebellion, revolution, insurrection, military or usurped power and civil war;

e) riot, commotion or disorder, except where solely restricted to employees of the Supplier.

11.2 **Effect of Force Majeure**

Neither party shall be considered to be in default or in breach of his obligations under the Contract to the extent that performance of such obligation is prevented by any circumstances of Force Majeure, which arise after the date of the Notification of Award.

11.3 **Notice of Occurrence**

If either party considers that any circumstances of Force Majeure have occurred which may affect performance of his obligations he shall notify the other party in writing of causes within fifteen (15) days from the occurrence of such a cause.

11.4 **Performance to Continue**

Upon the occurrence of any circumstances of force Majeure the Supplier shall endeavour to continue to perform his obligations under the Contract so far as reasonably practicable. The Supplier shall notify the Purchaser of the steps he proposes to take including any reasonable alternative means for performance, which is not prevented by Force Majeure. The Supplier shall not take any such steps unless directed so to do by the Purchaser.

11.5 **Additional Costs caused by Force Majeure**

If the Supplier incurs additional costs in complying with the Purchaser's directions under Sub-clause 11.4, the amount thereof shall be certified by the Purchaser and added to the Contract Price.

11.6 **Termination in Consequence of Force Majeure**

If circumstances of Force Majeure have occurred and shall continue for a period of 180 days then, notwithstanding that the Supplier may by reason thereof have been granted an extension of Time for Completion of the Works; either party shall be entitled to serve upon the other 30 days' notice to terminate the Contract. If at the expiry of the period of 30 days Force Majeure shall still continue, the Contract shall terminate.

11.7 **Payment on Termination for Force Majeure**

If the Contract is terminated under Sub-clause 11.6 the Supplier shall be paid the value of the work done.

The Supplier shall also be entitled to receive:

a) The amounts payable in respect of any preliminary items so far as the work or service comprised therein has been carried out and delivered and a proper proportion of any such item in which the work or service comprised has only been partially carried out and delivered.

b) The cost of the Services or for use in connection with the Services, which have been delivered to the Supplier or of which the Supplier is legally liable to accept delivery, such services shall become the property of and be at the risk of the Purchaser when paid for by the Purchaser and the Supplier shall place the same at the Purchaser's disposal.

c) The amount of any other expenditure, which in the circumstances was reasonably incurred by the Supplier in the expectation of completing the Services.

d) The reasonable cost of repatriation of the Supplier's staff and workmen employed wholly in connection with the Works at the date of such termination.

12.0 **Termination for Convenience**

12.1 The Purchaser, by written notice sent to the Supplier, 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 Purchaser's convenience, the extent to which performance of the Supplier under the Contract is terminated and the date which such termination becomes effective.

13.0 **Supplier's Default**

13.1 **Notice of Default**

If the Supplier is not executing the Works in accordance with the Contract or is neglecting to perform his obligations thereunder so as seriously to affect the programme for carrying out of the Works, the Purchaser may give notice to the Supplier requiring him to make good such failure or neglect.

13.2 **Nature of Supplier's Default**

If the Supplier

a) has failed to comply within a reasonable time with a notice under Sub-clause 13.1, or

b) assigns the Contract or subcontracts the whole of the Works without the Purchaser's written consent, or

c) becomes bankrupt or insolvent, has a receiving order made against him or compounds with his creditors, or carries on business under a receiver, trustee or manager for the benefit of his creditors or goes into liquidation.

The Purchaser may, after giving 30 days notice to the Supplier, terminate the Contract.

Any such termination shall be without prejudice to any other rights or powers of the Purchaser, or the Supplier under the Contract.

The Purchaser may upon such termination complete the Works himself or by any other Supplier. The Purchaser or such other Supplier may use for such completion any Supplier's equipment, which is upon the Site as he or they may think proper, and the Purchaser shall allow the Supplier a fair price for such use.

13.3 **Valuation at Date of Termination**

The Purchaser shall, as soon as possible after such termination, certify the value of the Works and all sums that are due to the Supplier as on the date of termination.

13.4 **Payment after Termination**

The Purchaser shall not be liable to make any further payments to the Supplier until the Works have been completed. When the Works are so complete, the Purchaser shall be entitled to recover from the Supplier the extra costs, if any, of completing the Works after allowing for any sum due to the Supplier under Sub-clause 13.3. If there is no such extra cost the Purchaser shall pay any balance due to the Supplier.

14.0 **Purchaser's Default**

14.1 **Nature of Purchaser's Default**

The Supplier may, by giving 30 days notice to the Purchaser, terminate the Contract if the Purchaser:

a) Consistently fails to pay the Supplier the amount due under payment certificates of the Purchaser within 30 days after the amount became payable, or

b) becomes bankrupt or insolvent, has a receiving order made against him, compounds with his creditors, or carries on business under a receiver, trustee or manager for the benefit of his creditors or goes into liquidation, or

c) Consistently fails to meet his contractual obligations.

Any such termination shall be without prejudice to any other rights of the Supplier or the Purchaser under the Contract.

14.2 **Removal of Supplier's Equipment**

On such termination, the Supplier shall be entitled to remove immediately all Supplier's Equipment/manpower, which is on the Site.

14.3 **Payment on Termination for Purchaser's Default**

In the event of such termination the Purchaser shall pay the Supplier an amount calculated in accordance with Sub-clause 11.7.

15.0 **Notices**

15.1 **Notices to Supplier**

All certificates, notices or written orders to be given to the Supplier by the Purchaser under these Conditions shall be sent by airmail post, facsimile transmission to or left at the Supplier's principal place of business or such other address as the Supplier shall notify for that purpose, or may be handed over to the Supplier's Representative.

15.2 **Minutes of Meetings**

Instructions or notices to the Supplier and notices from the Supplier to the Purchaser recorded in a minute or protocol signed by the authorised representative of the giver and of the recipient of such notice or instruction shall be valid notice or instruction for the purposes of the Contract.

16.0 **Arbitration**

16.1 If at any time any question, dispute or difference shall arise between the Purchaser and the Supplier in connection with or arising out of the Contract or the carrying out of the Works either party shall be entitled to refer the matter to be finally settled by arbitration in accordance with the following provisions:

16.2 In the event of the Supplier being an Indian party, that is to say a citizen and/or a permanent resident of India, a firm or company duly registered or incorporated in India, the arbitration shall be conducted by three arbitrators. One each to be nominated by the Supplier and the Purchaser and the third to be appointed as an umpire by both the arbitrators in accordance with the Indian Arbitration Act. If either of the parties fails to appoint its arbitrator within sixty (60) days after receipt of a notice from the other party invoking the Arbitration clause, the arbitrator appointed by the party invoking the arbitration clause shall become the sole arbitrator to conduct the arbitration.

16.3 The arbitration shall be conducted in accordance with the provisions of the Indian Arbitration & Conciliation Act, 1996 or any statutory modification thereof. The venue of arbitration shall be New Delhi, India.

16.4 In the event of foreign Supplier, the arbitration shall be conducted in accordance with the Rules of Conciliation and Arbitration of the International Chamber of Commerce by three arbitrators, one each to be appointed by the Purchaser and the Supplier and the third to be appointed by the Court of Arbitration of the International Chamber of Commerce, in accordance with the said "Rules". The arbitration shall be conducted at New Delhi, India. The language of arbitration shall be English.

16.5 The Arbitrator(s) shall have full power to open up review and revise :

a) any decision of the Purchaser referred to arbitration and

b) any certificate of the Purchaser related to the dispute.

16.6 The award given by the Arbitrator(s) under the Sub-clauses 16.2 & 16.4 shall be a speaking award.

16.7 **Works to Continue**

Performance of the Contract shall continue during arbitration proceedings unless the Purchaser shall order suspension. If any such suspension is ordered the reasonable costs incurred by the Supplier and occasioned thereby shall be added to the Contract Price.

No payments due or payable by the Purchaser shall be withheld on account of pending reference to arbitration.

16.8 **Time Limit for Arbitration**

Formal notice of arbitration must be given to the other party, and where required to the appropriate arbitration body no later than 90 days after the issue of the Final Certificate of Payment.

17.0 **Law and Procedure**

17.1 **Applicable Law**

The law, which is to apply to the Contract and under which the Contract is to be construed, shall be Indian law.

17.2 **Procedural Law**

The law governing the procedure and administration of any arbitration instituted pursuant to Clause 16.0 shall be Indian law.

18.0 **Taxation**

18.1 For service from abroad, the Supplier shall be entirely responsible for payments of all taxes, fees and other levies imposed outside the Purchaser's country and no liability on this account will accrue to the Purchaser whatsoever.

18.2 In case of services from within India, the Supplier shall be entirely responsible for payment of all taxes, duties, licence fees etc. incurred for the services to the Purchaser and no liability on this account will accrue to Purchaser's whatsoever.

18.3 The Supplier shall be solely responsible for the taxes that may be levied on the Supplier's persons or on earnings of any of his employees and shall hold the Purchaser indemnified and harmless against any claims that may be made against the Purchaser. The Purchaser does not take any responsibility whatsoever regarding taxes under Indian Income Tax Act, for the Supplier or his personnel. If it is obligatory under the provisions under the Indian Income Tax Act, deduction of Income Tax at source shall be made by the Purchaser.

18.4 The bidder shall include Service Tax and surcharge/cess etc. on it as applicable in their quoted bid price and the Purchaser would not bear any additional liability on this account. The Purchaser shall, however deduct such statutory taxes at source as per the rules and issue necessary certificate to the contractor.

18.5 The Bidder shall include the Sales Tax on Works Contract, Turnover Tax or any other similar taxes under the Sales Tax Act for services to be performed in Purchaser's country, as applicable in their quoted bid price and Purchaser would not bear any liability on this account. Purchaser shall, however, deduct such statutory taxes at source as per the rules and issue TDS Certificate to the Bidder.

18.6 No 'C' form shall be issued by ERLDC/POSOCO.

19.0 **Advertising**

19.1 Any advertising stating the subject of this Contract by the Supplier in India or in other foreign countries shall be subject to approval of the Purchaser prior to the publication.

Publication of approved articles, photographs and other similar materials shall carry acknowledgement of the Purchaser.

20.0 **Exception & Exclusions**

20.1 The provisions indicated above is a general guideline to be followed for execution of any contract being executed in POWERGRID / POSOCO.

20.2 However, any provision of the GCC if found in contradiction or not aligned with any of the provisions / scope laid down in Invitation for Bid (Section-I), Instruction to Bidder (Section-II), Special Condition of Contract (Section-IV) and Technical Specification (Section-V), the provisions in the later (i.e. the sections I /II/IV/V) shall prevail over the provisions laid down in this section.

21.0 Limitation of Liability

Notwithstanding anything contained herein, neither Party shall, in any event, regardless of the form of claim, be liable for any indirect, special, punitive, speculative, exemplary, consequential or incidental damages (including, without limitation, loss of use, data, revenue, profits, business), irrespective of whether it had an advance notice of the possibility of any such damages under this contract and the aggregate liability of the bidder, under this contract, shall not exceed the fees (excluding reimbursements) received by it under this contract during the six months preceding the date of such claim. Total Aggregate liability of the bidder for all claims shall not exceed the total fees received by them under this contract.

22.0 Settlement Of Disputes/Arbitration

All differences and/or disputes arising out of the contract shall be settled mutually but if required, the same would be resolved by arbitration as per the provision of the Arbitration & Conciliation Act 1996. G.M, ERLDC, POWER SYSTEM OPERATION CORPORATION LTD. shall be the sole arbitrator and if the G.M is unable or unwilling to act as the sole Arbitrator, some other person appointed by the Chairman & Managing Director, POWERGRID will be the Arbitrator. The award of the Arbitrator shall be final, conclusive and binding on all parties to the contract. The venue of the arbitration shall be such place as may be fixed by the Arbitrator. The cost of arbitration shall be borne by the parties to the dispute, as may be decided by the Arbitrator. The court of Kolkata shall have exclusive jurisdiction in all matters arising under the contract including execution of Arbitration awards.

POWER SYSTEM OPERATION CORPORATION LIMITED

Eastern Regional Load Despatch Centre

14 Golf Club Road, Tollygunge, Kolkata 700033

SECTION - IV

SPECIAL CONDITION OF CONTRACT

For

IMPLEMENTATION OF MANAGED IT SYSTEM SECURITY SERVICE

And

NETWORK THREAT MONITORING, DETECTION AND RESOLUTION SERVICES

At ERLDC

(E-TENDERING)

DOC Reference No. :	Issue Date:
ERLDC/C&M/1119/Antivirus etc/2016	**February 26, 2016**

A. TITLE OF THE PROJECT

Implementation of 100 users AV suite, Managed IT System Security Service and Network Threat Monitoring, Detection & Resolution Services at ERLDC.

B. INTRODUCTION

1.0 General Information

1.1 The following Special Conditions of Contract shall supplement the General Conditions of Contract. Whenever there is a conflict, the provisions herein shall prevail over those in the General Conditions of Contract.

1.2 The bidder can submit their bids only after getting bidding documents, duly authenticated by Power System Operation Corporation Limited's executive issuing the documents.

C. TERMS & CONDITIONS

1. Termination

Notwithstanding the duration of the agreement, owner shall have the right to terminate the agreement, without assigning any reasons whatsoever, by giving not less than 30 days notice in writing to the contractor, or its intention to terminate the same. In addition, POSOCO shall also have right to terminate this agreement forthwith on the happening of any of the following events:

1. If contractor commits breach of any of the terms and conditions mentioned in the contract documents.
2. If contractor commits any act which shall be prejudicial to the good name or interest of our company.
3. If contractor's firm is adjudged insolvent or any of contractor's partner commits any act of insolvency or a compromise is entered into by contractor / its partner with your creditors or if a distress execution or other process is levied upon property and assets or those of partner.
4. If for any act of contractor, POSOCO comes to the conclusion that it is not in our interest to continue with contractor's services.
5. POSOCO shall have the right to terminate the contract after giving notice of one month if the availability of the system is not attained as per specification consecutively for two months or availability of suitable manpower as per satisfaction of the POSOCO representative is not maintained with adequate skill set for resolving day to day problems reported for one month or more in continuation or discrete.

2.0 Liability For Loss or Damage to Property

Any loss or damage to the equipments during carrying out maintenance activities shall be to the account of the contractor. The contractor shall be responsible for making good the damages or loss by way of repair and/or replacement of the equipment, damaged or lost. This shall be applicable for cases where any physical damage has occurred is due to any maintenance activity and/or mal-operation of the personnel deputed the same shall not be limited by the limitation of liability clause (refer cl.D4.0 of IFB). Loss of data and system integrity occurrences during fault rectification process shall not be covered under this clause and shall be guided by the provision of Limitation of liability clause referred above.

3.0 **Performance Security**

The Performance Security shall be equivalent to an amount of 10% of the Contract Price.

4.0 **Confidentiality**

The Bidder will be exposed, by virtue of the contracted activities, to internal business information of POSOCO, affiliates, business partners and /or customers. The bidder would be required to provide an undertaking that they will not use or pass to anybody the data/information derived by virtue of execution of this contract in any form. The bidder must safeguard the confidentiality of POSOCO, applications and data. For this bidder and his employees are required to sign Non-disclosure agreement with POSOCO.

Disclosure of any part of the afore mentioned information to parties not directly involved in providing the services requested, unless required to do so by the Court of Law or other Statutory Authorities, could result in premature termination of the contract. POSOCO may apart from blacklisting the bidder, initiate legal action against the bidder for breach of trust. The bidder shall also not make any news release, public announcements or any other reference on the development or contract without obtaining prior written consent from the POSOCO.

5.0 **Obligations of the Bidder**

5.1 The Bidder shall, in accordance with the Contract, with due care and diligence, carry out the Works as per the scope of work defined in the Specifications and Scope of work and within the specified Time. The Bidder shall also provide all necessary Bidders' equipment, superintendence, labour and all necessary facilities thereof.

The Bidder shall be deemed to have carefully examined the Bidding Documents, and to have satisfied himself to the nature and character of the Work to be executed, the prevailing meteorological conditions as well as the local uses and conditions and any other relevant matters and details.

5.2 The Bidder shall acquire all necessary permits, approvals and/or licences that are necessary for the performance of the Contract if not specifically excluded from the scope of this contract.

5.3 The Bidder shall comply with all laws in force in the Purchaser's country where Services are to be carried out. The laws will include all national, provincial, municipal or other laws that affect the performance of the Contract and bind upon the Bidder. The Bidder shall indemnify and hold harmless the Purchaser from and against any and all liabilities, damages, claims, fines, penalties and expenses of whatever nature arising or resulting from the violation of such laws by the Bidder or its personnel, including the Sub-suppliers and their personnel.

पावर सिस्टम ऑपरेशन कॉरपोरेशन लिमिटेड

POWER SYSTEM OPERATION CORPORATION LIMITED

पूर्वी क्षेत्रीय भार प्रेषण केन्द्र

Eastern Regional Load Despatch Centre

14 Golf Club Road, Tollygunge, Kolkata 700033

TECHNICAL SPECIFICATION (TS)

For

IMPLEMENTATION OF MANAGED IT SYSTEM SECURITY SERVICE

And

NETWORK THREAT MONITORING, DETECTION AND RESOLUTION SERVICES

At ERLDC

SECTION - V

DOC Reference No. :	Issue Date:
ERLDC/C&M/1119/Antivirus etc/2016	**February 26, 2016**

Table of Contents

1. Title of the Project

Implementation of Managed IT System Security Service and Network Threat Monitoring, Detection & Resolution Services at ERLDC.

2. Scope of work

Power System Operation Corporation Limited, Eastern Regional Load Despatch Centre in its office at 14, Golf Club Road intends to implement suitable intelligent real-time security management service for its IT establishment. The services essentially includes design, engineering, supply, installation and configuration of suitable Hardware device for continuous monitoring and vulnerability assessment & penetration testing of the IT establishment at ERLDC and further undertake periodic remedial action towards closure of all security threat findings. The scope of the service also includes generation of necessary reports, patch management, Antivirus Management, undertaking Preventive Action, Root Cause Analysis, Correction and Corrective action of all security incident, accident and near misses and also to maintain adequate logs & records of all such events with information related to change management, security management and monitoring and analysis of effectiveness of controls as per ISO27001:2013 Standard requirement.

In pre-implementation stage the scope shall include assessment of current Network security architecture available at ERLDC for protecting information systems and business critical applications and hardware installations. Further, the bidder shall also conduct a gap analysis to ascertain pain areas in comparison to industry standards and POSOCO Security policy & procedure. Design & Engineering of the proposed security architecture should be based on the findings of the gap analysis and to fulfill the requirement as specified in this technical specification in its true spirit & sense not limited by the specific features and/or technical datasheet.

The scope of the work includes design, engineering, handling, insurance, loading unloading, packing, forwarding, delivery at site, installation at identified locations, testing and commissioning and system integration with the existing setup up to the satisfaction of the consignee suitable Hardware device in conformance but not limited to the technical specification given herewith which is capable of providing sufficient information regarding external & internal advanced persistent threats prevailing in the ERLDC IT setup and also provide adequate support to the management team towards monitoring, record buildup and resolution of such threats. The scope necessarily includes all such items & services required to meet the desired objective of the entire tender in line with the industry practice and standard of Service Level Agreement towards system availability, uptime and other objective parameters followed at Data Centre installations in general.

The scope other than supply, installation & commissioning of the Anti-APT Hardware and associated software also includes supply of Client-Server Based Anti-Virus / Anti-Spam & Anti-Malware protection suite for 100 users valid for 3 years. It is preferable that for ease of manageability & integration the AV suite & Anti-APT solution belong to same OEM and is inter-operable.

The equipment shall be complete in every respect with all mounting, fittings, fixtures and standard accessories such as adapter, cable manager etc. needed for installation and safe operation of the system at the pre-identified location, though some of them may not have been detailed in this

technical specification. Necessary integration of the system in the ERLDC Network shall be within the scope of the contract. Proper care must be ensured for maintaining the aesthetic of the Server room as well as the building as a whole un-tampered during installation.

The system should have field proven design for continuous operation. The equipment shall operate safely without any undue sag, heating, vibration, noise, electromagnetic interferences or similar problems. Supplier must warrant that the supplied products will operate to the standards and specifications claimed by the manufacturer. In the event that the supplied products fail to satisfy this requirement, supplier must supply replacement items at no extra cost.

The supplier must confirm availability of spares and maintainability of the supplied system along with all other accessories and associated equipment for a period of at least 5 years after expiry of warranty period. The supplier shall be ready to provide additional hardware as suitable for future expansion of the system if required at a mutually agreed rate. The supplier shall be ready to provide comprehensive annual maintenance and security management service even after completion of the present scope for at least another 3 years at a rate to be agreed mutually but not exceeding the present rate (AMC & Service portion only) by 10-15% per year thereafter. The attendance and rectification of fault within 24 hours of reporting shall be ensured. Periodic monitoring, reporting and patch management along with action towards closure of all reported vulnerabilities as per pre-defined schedule (indicated in relevant section below) should be considered within the scope of contract. This also essentially includes deputation of suitably skilled manpower on regular basis for security management purpose at ERLDC premises during office hours. Also, maintenance of necessary spares (if any) to ensure minimum downtime should be considered within the scope of the contract. The replaced spare shall be the property of the supplier under warranty period.

The supplier shall also be responsible for the overall coordination with internal external agencies, project management and training of purchaser's manpower, loading, unloading, handling and movement of equipment / materials to final destination, storing prior to successful erection, testing and commissioning of the system. The bidder will conduct half-yearly third party audit to ensure effectiveness of the security management system implemented and maintained. The vendor should extend all support during the third party security audit as well as ISMS certification audit conducted by BSI. Effectiveness of the security management system will be measured based on the third party audit and release of payment for the service portion shall be partially linked with the third party audit findings.

Any other items not specifically mentioned in the specification but which are required for erection, testing & commissioning & satisfactory operation of the works are deemed to be included in the scope of the specification unless specifically excluded.

The offered system must be capable of further expansion both functionally and in size, simply and cost-effectively by the addition of required compatible modular devices.

3. Hardware Technical Specification

The proposed hardware device should be integrated within the ERLDC LAN and should be capable of monitoring both internal and external threats. The network to be considered for provision of the

security management service includes ERLDC LAN boundary and its connectivity with other LAN / WAN Zones and public domains. A detailed Network Diagram showing existing setup is attached herewith at Annexure A.

The proposed hardware should be one among the leading models available in the market proven to provide desired protection against Targeted Attacks and Advanced Persistent Threats.

The Hardware should use advanced protection platform such as "Deep Discovery threat protection platform" or similar which detects, analyse, and respond to today's stealthy, targeted attacks in real time. Deployed as individual components or as a complete cyber security platform, the system should provide advanced threat protection with 360-degree network monitoring of all traffic to detect all aspects of a targeted attack. Integrated Specialized detection engines and custom sandboxes should be there to identify and analyse malware, command-and-control (C&C) communications, and evasive attacker activities that are invisible to standard security defences. In-depth threat intelligence enabling rapid response should be provided which in turn should be shared automatically with other implemented security products to create a real-time custom defence against attackers. The evaluation process should be able to detect and report on both malicious content and malicious communications through monitoring network communications at one or more ingress/egress points in POSOCO's network.

Focus on identifying malicious content, communications, and behaviour indicative of advanced malware or attacker activity across every stage of the attack sequence, using a non-intrusive, listen-only inspection of all types of network traffic should be available. Advanced Threat Scan Engine in general should use a combination of signature file-based scanning and heuristic rule-based scanning to detect and document exploits and other threats used in targeted attacks. Further, engine like Virtual Analyser should be available using sandbox simulation to provide additional detection and full forensic analysis of suspect content. Smart Protection Network intelligence and dedicated Threat Researchers providing continually updated detection intelligence and correlation rules to identify attacks must be available with the OEM. Real time threat console should also be available to provide geographic origins of malicious communications. Feature to provide the intelligence needed to understand and remediate an attack also should be present which should give direct access to OEM's intelligence portal for a specific attack or malware.

Through detection and in-depth analysis of both advanced malware and evasive attacker behaviour, the system should provide IT establishment of ERLDC with a new level of visibility and intelligence to combat APTs and targeted attacks across the evolving computing environment.

3.1. Key Features

Comprehensive threat detection: Should be capable of monitoring all ports covering more than 80 protocols to identify attacks anywhere within the network.

Detect malware, C&C, attacker activity: Should use specialized detection engines, correlation rules, and custom sandboxing (or similar technology) to detect all aspects of a targeted attack, not just malware.

Custom sandboxes: Should use images that precisely match ERLDC system configurations to detect the threats that are targeted to this organization.

Broad system protection: Detects attacks against Windows, Mac OS X, Android, Linux, and any system.

Single appliance simplicity and flexibility: Simplifies security management with a single appliance available in a range of capacities, deployable in hardware.

Integrate Into Any Environment: Shares indicators of compromise (IOC) with most third-party products and services such as firewalls, Check Points, and others IDMs to have proactive corrections.

The features indicated above are indicative and desired. However, all care should be taken in designing the product keeping in mind the intrinsic desire of the scope and necessary solution thereof. Further also an indicative threat vs. discovery mechanism is tabulated below for reference and guideline in selection of the product.

	Attack Detection	Detection Methods
Advanced Malware	✓ Zero-day & known malware ✓ Emails containing embedded document exploits ✓ Drive-by downloads	✓ Decode & decompress embedded files ✓ Custom sandbox simulation ✓ Browser exploit kit detection ✓ Malware scan (signature and heuristic)
C&C Communication	✓ C&C communication for all malware: bots, downloaders, data stealing, worms, blended threats, etc. ✓ Backdoor activity by attacker	✓ Destination analysis (URL, IP, domain, email, IRC channel, etc.) via dynamic blacklisting, white listing ✓ Smart Protection Network reputation of all requested and embedded URLs ✓ Communication fingerprinting rules
Attacker Activity	✓ Attacker activity: scan, brute force, tool download, etc. ✓ Data exfiltration ✓ Malware activity: propagation, downloading, spamming, etc.	✓ Rule-based heuristic analysis ✓ Extended event correlation and anomaly detection techniques ✓ Behaviour fingerprinting rules

Detection & Protection against following attacks are desired:

- ✓ APTs and targeted attacks
- ✓ Zero-day malware and document exploits
- ✓ Attacker network activity
- ✓ Web threats (exploits, drive-by-downloads)
- ✓ Email threats (phishing, spear-phishing)
- ✓ Data exfiltration
- ✓ Bots, Trojans, Worms
- ✓ Key Loggers and Crime ware
- ✓ Disruptive applications

Anti-Malware Protection

- ✓ Should deliver an anti-malware agent to extend protection to physical and virtual servers
- ✓ Should be capable of Optimizing security operations to avoid antivirus storms commonly seen in full system scans and pattern updates
- ✓ Should provide Tamper-proofs security from sophisticated attacks in virtual environments by isolating malware from anti-malware

Bidirectional Stateful Firewall

- ✓ Decreases the attack surface of physical, cloud, and virtual servers with fine-grained filtering, design policies per network, and location awareness for all IP-based protocols and frame types
- ✓ Should be featured with centrally managed server firewall policy, including templates for common server types
- ✓ Should prevent denial of service attacks and be capable of detecting reconnaissance scans

Intrusion Detection and Prevention

- ✓ Should protect against known and zero-day attacks by shielding known vulnerabilities from unlimited exploits
- ✓ Should have feature to examine all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack
- ✓ Should automatically shield newly discovered vulnerabilities within hours, pushing protection to thousands of servers in minutes without a system reboot
- ✓ Should include out-of-the-box vulnerability protection for all major operating systems and over 100 applications, including database, web, email, and FTP servers

Smart In-the-cloud protection platform with Virtualization awareness

Platforms like Office-Scan delivering comprehensive protection for virtual and physical desktops on and off the corporate network should be featured with. Further, anti-malware protection with in-the-cloud protection from OEM Protection Network support should be provided to equip the proposed solution to defend against high volumes of new threats.

Virtualization awareness ensuring constant availability by eliminating resource contention issues caused by conventional security on virtual desktops also is desired. Features like File Reputation to further liberating the resources by moving the burden of pattern file management into the cloud and Intrusion Defence Firewall plug-in to provide virtual patching thereby protecting against zero-day threats before patching should be possible.

3.2. Desired Technical Data Sheet

S/N	Functional Features
1.0	***General Specs***
1.1	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections.
1.2	The proposed solution should support the native CEF,LEEF format for SIEM log integration

S/N	Functional Features
1.3	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.
1.4	Proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network
1.5	Upon detection of the threat, the proposed solution should be able to perform behaviour analysis for advance detection
1.6	Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.
1.7	Solution should provide risk based alerts or logs to help prioritize remediation effort
1.8	Solution should be deployed on premise along with on premise sandboxing capability
1.9	The proposed solution should be able to store payload of the detected threats
1.10	Solution should have ability to interrupt malicious communication
1.11	Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth
1.12	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment.
1.13	Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation an attack.
1.14	Solution deployment should cause limited interruption to the current network environment.
1.15	The proposed solution should able to work with the existing technologies for advance threat protection through web protocol
1.16	The proposed solution should allow organization to gain visibility to the internal networks and flag detected threats immediately
1.17	The proposed solution should have the ability to support out-of-band detection
1.18	The proposed solution should be able to detect (lateral moments) movement of the attacker and the attacks within organization's network
1.19	The proposed solution should not have any port based limitation and should support all ports.
1.20	The proposed solution should support at least 100+ protocols for inspection. Example :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction :SMB ,Database protocol (MySQL, MSSQL, Oracle)
1.21	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.
1.22	The Proposed solution should be able to support up to 5 network segments on a single appliance.
1.23	The proposed solution should be able to detect any suspicious communication within and outside of ERLDC network
1.24	The Proposed solution should be able to detect communications to known command and control centres

S/N	Functional Features
1.25	The proposed solution should be able to detect reputation of url being accessed
1.26	The proposed solution should be able to identify and help ERLDC to understand the severity and stage of each attack
1.27	The proposed solution should have built in capabilities to add exceptions for detections
1.28	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list
1.29	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis.
1.30	The Proposed solution must have capabilities to correlate the detections on the device itself.
1.31	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal
1.32	The Proposed Solution should be able to contain, remediate and quarantine the threats on the all the endpoints of the organization
2.0	***Malware Analysis***
2.1	Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviours for advanced threat detection.
2.2	The proposed solution should be able to provide customizable sandbox to fulfil ERLDC's environments and needs.
2.3	Sandbox must supports multiple operating systems and for both 32-bits and 64-bits OS
2.4	Solution must have the capability to analyse large files. Must be able to support more than 40MB file size
2.5	Sandbox must have the ability to simulate the entire threat behaviour. i.e. honeynet and honeypot framework
2.6	The Proposed solution should support windows XP, Windows 7, Windows 8, Microsoft 2003 and Microsoft 2008 operating environments for Sandboxing
2.7	The proposed solution should have grey ware detection capabilities.
2.8	The proposed solution must provide a web service interface/API for Customer to customize their system integration.
2.9	The Proposed solution should be able to detect Network Attacks and Exploits.
2.10	The proposed solution should have capability to scale out the detection when the bandwidth increase in future
2.11	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp
2.12	The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.
2.13	The proposed solution must provide the capability to exportable network packet files and encrypted suspicious files for further investigation.

S/N	Functional Features
2.14	The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files
2.15	The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing
2.16	The proposed solution should have capabilities to scan inside password protected Archives
2.17	The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms
2.18	The proposed solution must have capabilities to detect Mac and mobile malwares
2.19	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list
2.20	The proposed solution should have capability to include User-defined and context-derived passwords for protected archives
2.21	The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.
2.22	The Proposed solution should be able to detect known malwares before sending suspicious files to Sandbox for analysis
2.23	The Proposed solution should be able to correlate local APT attacks with Global historical APT attacks.
2.24	The Proposed solution should support at least 1Gbps of throughput
2.25	The Proposed solution should have usable storage of 500GB
2.26	The Proposed solution should support at least 4x10/100/1000 Ethernet Interfaces
3.0	***Report***
3.1	The proposed solution should have an intuitive customisable Dashboard that offers real time threat visibility and to provide Investigative dashboard that is capable of displaying correlated graphical data that is based on link-graph, geo-map, chart, tree-map/pivot table etc.
3.2	The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats
3.3	The proposed solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time)
3.4	The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attacks sessions.
3.5	The proposed solution should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.
3.6	The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable

S/N	Functional Features
3.7	The proposed solution should be able to integrate with the existing endpoint, web and email management solutions at Customer for further detailed reporting.
3.8	The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.
3.9	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behaviour, Lateral Moment, Asset and data discovery and Exfiltration
4.0	***Authentication Administration and Configuration Requirement***
4.1	The proposed solution shall support Local Password authentication schemes
4.2	The proposed solution shall support Remote administration using SSH/HTTPS
4.3	The proposed solution shall support CLI, GUI/Web based Administration Console.

The Data-sheet given is indicative for the desired technical details and if resembles with any single Make/Model is unintentional. Any proprietary protocol (if indicated) may be ignored.

4. Anti-virus / Anti-Spam / Anti-Malware Security Suite Datasheet

3 (three) years 100 (one Hundred) Users License AV Protection Suite of reputed make (preferably same OEM as that of the Anti-APT solution proposed) should be provided and suitably installed at designated Desktop / Laptop & Servers as per satisfaction of the consignee representative. Manageability of the AV suite for its 3 (three) year life shall be within the scope of this contract.

A detailed data-sheet indicating preferred features of the AV Suite is tabulated below:

S/N	Functional Features
	Antivirus Protection and Other features
1	Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.
2	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.
3	Must include capabilities for detecting and removing rootkits
4	Must provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution
5	Must have capabilities to restore spyware/grayware if the spyware/grayware is deemed safe
6	Must have Assessment mode to allow first to evaluate whether spyware/grayware is legitimate and then take action based on the evaluation
7	Must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process
8	To address the threats and nuisances posed by Trojans, the solution should be able to do the following:
8.1	Terminating all known virus processes and threads in memory
8.2	Repairing the registry
8.3	Deleting any drop files created by viruses
8.4	Removing any Microsoft Windows services created by viruses

S/N	Functional Features
8.5	Restoring all files damaged by viruses
8.6	Includes Clean-up for Spyware, Adware etc.
9	Must be capable of cleaning viruses/malware even without the availability of virus clean-up components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether
10	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients in case there is an outbreak
11	Behaviour Monitoring: Must have behaviour monitoring to restrict system behaviour, keeping security-related processes always up and running and enable Certified Safe Software Service to reduce the likelihood of false positive detections
12	Must provide Real-time clock down of client configuration – allow or prevent users from changing settings or unloading/uninstalling the software
13	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.
14	CPU usage performance control during scanning:
14.1	Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer
14.2	Adjusts the scanning speed if:
14.2a	The CPU usage level is Medium or Low
14.2b	Actual CPU consumption exceeds a certain threshold
15	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually
16	Should have Integrated spyware protection and clean-up
17	Should have the capability to assign a client the privilege to act as a update agent for rest of the agents in the network
19	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
20	Safeguards endpoint mail boxes by scanning incoming POP3 email and Outlook folders for Threats
21	shall be able to scan only those file types which are potential virus carriers (based on true file type)
22	Should be able to detect files packed using real-time compression algorithms as executable files.
23	Solution should be able to manage both SaaS and on premise solution from the single management console
24	Client machine acting as update agent which is delivering pattern updates to rest of the machines in the LAN, should have the capability to upgrade program upgrades also. No separate web server should be required
25	Should have a provision for setting up a local reputation server so that for verifying reputation of any file, endpoints should not contact Internet always.
26	shall be able to scan Object Linking and Embedding (OLE) File
Manageability and integration	
1	Must provide Comprehensive Support for Network Admission Control
1.1	Should be able to deploy the Client software using the following mechanisms:
1.2	Client Packager (Executable & Microsoft Installer (MSI) Package Format)

S/N	Functional Features
2	Web install page
2.1	Login Script Setup
2.2	Remote installation
2.3	From a client disk image
2.4	Support MS Systems Management Server (SMS)
2.5	Must provide a secure Web-based management console to give administrators transparent access to all clients and servers on the network
2.6	The management server should be able to download updates from different source if required, which could be the vendor's update server, any other server or a UNC path
3	If the update from the Management server fails, the security clients with the privilege should be able to get updated directly from the vendor's server
4	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns
5	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console
6	Should have role based administration with active directory integration
7	To create custom role type
8	To add uses to a predefined role or to a custom role
8.1	Should have integration with the Active directory
8.2	Shall support grouping of clients into domains for easier administration
9	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)
10	Shall offer centrally managed Client Firewall and IDS
11	Must be capable of uninstalling and replacing existing client antivirus software (Provide the detailed list)
12	Must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capabilities to clients and servers across the network
14	Security Compliance leverages Microsoft Active Directory services to determine the security status of the computers in the network
	Platform Support
1	Windows XP SP3 32-bit Edition
2	Windows 2003 32-bit Edition
3	Windows XP/2003 64-bit Edition
4	Windows Vista (32-bit & 64-bit)
5	Microsoft Windows Storage Server 2003
6	Windows 7, 32-bit version & 64-bit version
6	Microsoft Cluster Server 2003
7	Windows Server 2008 and Windows Server 2008 R2, 64-bit version
8	client installation on guest Windows 2000/2003/2008 operating systems hosted on the following virtualization applications:
8.1	VMware ESX/ESXi Server 3.5 or 4 (Server Edition)
8.2	* VMware Server 1.0.3 or later (Server Edition)
8.3	* VMware Workstation and Workstation ACE Edition 6.0
9	Should support Intel x64 processor & AMD x64 processor
10	Should support wireless devices such as Palm, Pocket PC, and EPOC at no extra cost

S/N	Functional Features
11	Virtual Desktop Support : Solution should support Virtual Desktop for the following platforms:
11.1	· VMware vCenter™ 3.5 and 4 (VMware View™ 4)
11.2	· Citrix™ XenServer™5.5 and 5.6 (Citrix Xen Desktop™ 4)
	Notification, Reporting and logging
1	Must be able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via E-mail, Pager, SNMP trap or Windows NT Event log
	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from IDS, personal firewall, and/or network virus logs exceed certain thresholds, signalling a possible attack.
2	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from personal firewall, and/or network virus logs exceed certain thresholds, signalling a possible attack.
3	"Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack
4	Shall offer customizable & standard notifications via - SMTP, SNMP, Pager, NT Event Log with No additional agent to be deployed at endpoint
5	Protect Data at rest, in use, and in Motion
6	Product should be integrated with Gateway URL Filtering/Proxy Server and Endpoint Antivirus with no addition agent deployment
7	Detects and reacts to improper data use based on keywords, regular expressions and file attributes
8	Educates employees on corporate data usage policies through alerts, blocking and reporting
9	Empowers IT to restrict the use of USB drives, CD/DVD writers, and other removable media
10	Offers granular device control, including the ability to create specific rules based on make and serial number of the device
11	Reduces resource demand and performance impact with a single agent for endpoint security and data loss prevention
12	Tracks and documents sensitive data flowing through network egress points
13	Detects and reacts to improper data use based on keywords, regular expressions and file attributes
14	Simplifies deployment with a data loss prevention plug-in, requiring no additional hardware or software
15	Improves visibility and control with a fully-integrated, centrally managed solution
16	Automates response to policy violations with options to log, bypass, block, encrypt, alert, modify, quarantine, or delete data : Data at rest with wide coverage of file types, Data in motion control points, Data in use control points

The Data-sheet given is indicative for the desired technical details and if resembles with any single Make/Model is unintentional. Any proprietary protocol (if indicated) may be ignored.

5. Security Management Service & Remedial Measures

The scope of this contract essentially also includes provision of Security management Service and undertaking remedial measures to ensure imposition of adequate security mechanism at all times.

The scope covers deployment of suitably skilled manpower at ERLDC premises to suitably configure & manage the installed hardware, ensuring proper patch management and also to provide necessary support in protecting the system from all possible threats & attacks.

This also includes the following services:

Generation of periodic report viz. Weekly, Monthly & Quarterly report on IT resource utilisation, possible vulnerabilities & threats, reports of intrusions & remedial measures taken thereof. The scope of documentation also will include but not limited to all such reports such as patch management records, Anti-virus management records, Change management records, Risk Assessment-Risk Treatment & Mitigation plan record, Preventive Action records, IT Incident management, correction, root cause analysis and corrective action records etc. in conformance with the IT security policy and in line with the ISO 27001:2013 standard requirements.

Ensuring remedial action towards risk & threats: In an APT scenario two strategies are most important viz. remediation and containment. Based on which stage of APT is detected, the strategy of containment and remediation should be decided. These may be further named as correction (i.e. containment to spread further) and corrective action (i.e. Remediation measure). The scope essentially includes immediate correction of any threat detected by the vendor. All necessary action in hardening, segregation of faulty section (if required), rectification and restoration of the system in normalised state should be in the scope of the vendor. On restoration the system should be further tested to ensure effectiveness of the hardening implemented.

Option for smart feedback to the appliance OEM is desired so that for binary (PE) files, the same is submitted to the OEM research team for creation of new signatures & update in form of patch. For any zero-day threat necessary correction may be taken up immediately and further assistance from OEM may be seek for corrective action.

Periodic VAPT (on monthly basis) other than continuous real-time monitoring by the hardware appliance should also be featured in the scope of contract to ensure adequate preventive monitoring & action.

Third party Audit preparation, participation & support: effectiveness of the security management service shall be assessed through third party security audit to be conducted by ERLDC selected third party auditor. The vendor's scope in this connection restricts to provide all necessary support to the auditor during his audit process. Further, CAV or Recertification audit process involved in BSI / Internal Auditor's audit for compliance with ISMS standard also should be supported by the vendor. The scope of this contract also essentially includes implementation and closure of all findings and recommendation arising from all such audits.

Deployment of Manpower: the vendor should deploy suitably skilled manpower as per desired qualification indicated below at ERLDC premises as per desired requirement to ensure proper security management service, monitoring and remedial actions. The responsibility of such personnel deployed will be to ensure proper implementation, assessment, monitoring & remediation of the IT system security measures at ERLDC encompassing 360 degree coverage in truest intent and spirit not limited to the specific scope detailed here. However, provision of any third party tool, service or

support required time-to-time as system strengthening to ensure continual improvement to ensure sustainability shall be within the scope of the bidder (ERLDC).

Qualification & Experience of Front Level Security Engineer (responsible for routine security management activity): Graduate with min 5 years of experience in handling security devices in complex network environment. Should have product specific Security Certificates like TCSA, FCNSP, CCSE, CCNSP, etc. Should have Network Certification like CCNA.

Qualification & Experience of Expert Level Security Engineer (responsible for analysis & corrective action in abnormal / critical situation): Graduate with min 10 years of industry experience. Must have experience in resolving critical security issues, analysing cyber threats and combat cyber-attack. Must have implemented similar product in last two years. Should have product specific security certificates like TCSE, FCNSP, CCSE, CCNSP, etc. Should have network certification like CCNA.

Profile of Delivery Head (responsible for overall service delivery, security trend analysis, aligning the security activities with ISO 27001): BE /B.Tech / MCA with min 15 years of work experience. Must have managed similar projects in complex network environment. Should have experience in escalation handling and Incident Management. Should have product specific certificates and additional certificates like CCNA, CEH, ITIL, ISO 27001:2013 Lead Auditor (preferable).

Documentation: Maintenance of adequate documents & records to support the security measures implemented and monitored an also to ensure proper analysis towards continual improvement is the essence of any security system implementation. Preparation of all necessary documents in desired frequency and as per pre-defined formats as per ERLDC ISMS policy & procedure and as required in implementation of suitable security management system should be considered within the scope of the contract.

6. Additional Features

It should be noted that design information and bill of quantity are provisional only. The Contractor shall verify the design data during the site surveys & detail engineering and finalise the BOQ as required for ultimate design & system performance to fulfil the scope. The Bidder's proposal should address all functional and performance requirements within this specification and should include sufficient information and supporting documentation in order to determine compliance with this specification without further necessity for enquiries.

The Bidder's proposal shall clearly identify deviation from technical specification if any; i.e. deviation from all those features which are described in the specifications or in any supporting reference material, which will not be implemented or has been considered by the bidder as exclusion from bidders scope; otherwise, those features shall become binding as part of the final contract.

An analysis of the functional and performance requirements of this specification and/or site surveys, design, and engineering may lead the Contractor to conclude that additional items and services are required that are not specifically mentioned in this specification. The Contractor shall be responsible for providing at no added cost to the Employer, all such additional items and services

such that a viable and fully functional System is implemented that meets or exceeds the capacity, and performance requirements specified. Such materials and services shall be considered to be within the scope of the contract. To the extent possible, the Bidders shall identify and include all such additional items (hardware / software) and services in their proposal.

All equipment provided shall be designed to interface with existing equipment and shall be capable of supporting all present requirements and spare capacity requirements identified in this specification. The required connectors/cabling for interface with the existing communication equipment shall be in the scope of the contractor.

The Computer hardware and software at ERLDC shall be designed and provisioned for 100 % expansions and reconfigurations without impairing normal operation. The bidders are advised to visit ERLDC site (at their own expense), prior to the submission of proposal, and make surveys and assessments as deemed necessary for proposal submission.

7. Duration of Service

The hardware supplied should have warranty / support coverage for 3 (three) years from date of successful installation & commissioning & issuance of TOC. The Security Management Service also shall presently include 3 (three) years support service from date of TOC. All Hardware, Software & Service scope shall continue for the said 3 (three) years period.

8. Software

The desired scope includes generation of reports regarding various monitored parameters as indicated above. All software required to achieve the desired feature should be considered as inclusive in the scope of this contract. Any embedded / add on operating software(s) if required for managing and controlling the basic features of the system / scope in various modes of operation must be supplied along with the system at no extra cost and must be user friendly in use. Licensing & support for all such software (if not perpetual) must be at-least for 3 (three) years from date of TOC.

9. Other Non-functional Requirements

Performance Requirements

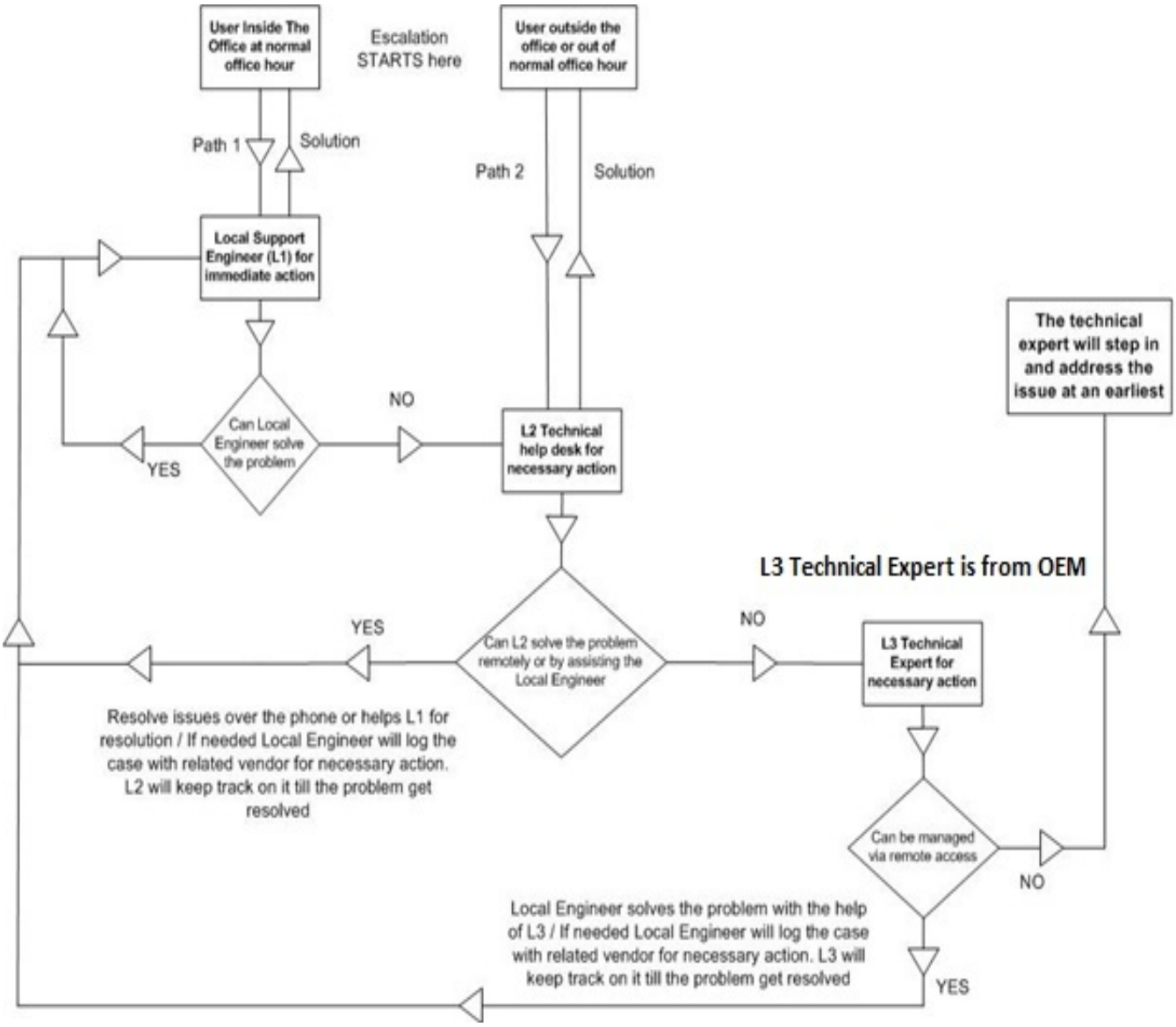
The system should be operational round the clock. Multiple users should be able to access the system at the same time. The processing speed depends on machine speed and other network parameters. It should work satisfactorily on Pentium family processors.

Security Requirements

Necessary Logs for all the processes and activities done by any member to be maintained and be made available to the System Administrator.

Standard Service Escalation Matrix

Resolution of service calls should be systematic and suitably recorded. Necessary infrastructure to smoothly report and resolve any service call and security incidences must be implemented by the vendor. A schematic call-resolution matrix is depicted hereunder for ease of understanding.



10. Training

The vendor shall provide 3 days administrative level training by engaging OEM certified trainer on the various features and management of the Anti-APT solution provided along with management of the entire system. Suitable training kit with all necessary documents / literature must be provided during the training. The training may be arranged at Vendor's preferred location / at ERLDC on a mutually agreed date for at least 5 participants.

Arrangement of training material, faculty, other logistics, refreshments etc. during the training should be within the scope of the contract at no extra cost.

11. Acceptance Criteria

It should meet all the basic functional requirements mentioned in functional requirements in the SRS. The test procedures (SAT documents) shall be prepared by the vendor for all the modules and

submitted for approval by RLDC for acceptance. The test shall be carried out for verification and acceptance of the software.

12. System Integration, Configuration, Smooth Migration and Maintenance

Scope of the project includes installation at designated location / system, configuration and smooth integration of the various supplied products (both Hardware and software) so that the desired Security Management service as per designed architecture and technical specification can be obtained. Further, trouble free and smooth migration of the existing system to the new system with minimum possible down-time must be ensured and considered within the scope of the project.

The scope also includes necessary configuration, scheduling and activation of Anti-ATP and AV solution to facilitate scheduled, periodic VAPT encompassing 360 degree coverage and signature update at all client machines, VMs, Servers, Oracle database etc. as well as to facilitate centralised management, reporting & other relevant activity.

Further, as all the supplied equipment are covered under warranty or support subscription for 3 years, the vendor shall be providing suitable maintenance of the system for 3 years from date of successful installation and taken over by ERLDC. During the maintenance period the vendor shall be responsible for:

- All sort of troubleshooting for the entire system/setup as whole as well as do necessary configuration, modifications, alteration and/or administration of the existing setup to accommodate requirements like integration of new elements, configuration changes etc.
- Co-ordination with the OEM or other third party for timely support and service of the supplied products during the maintenance / support period to ensure system availability of more than 99.999%.
- Co-ordinate with the OEM for installation, configuration and trouble free operation of patch / updates published by the OEM time to time for all the products supplied within the scope of support.
- Facilitate single window call-logging / fault reporting system for 24 x 7 basis through web portal or phone calls. Also necessary call-logs with resolution time details to be maintained.

The vendor shall submit all documents pertaining to licenses, system configurations, drawings, troubleshooting charts, management user manual etc. at the time of commissioning to ERLDC representative and also shall maintain change management documents during the maintenance period. Any service requirement should be addressed within 3 hours if the same is resulting in total / partial system failure. It is the responsibility of the vendor for receiving the first hand call and further coordinating with the OEM for suitable resolution. Call resolution indicates total down time of the system or part thereof from call reported till bringing the system up & running.

Generation of reports, correction & corrective actions etc. should be provided as per pre-decided periodicity to be mutually agreed. Suitable deduction from CPG / SD and Maintenance charges may be applied for non-adhering to the above conditions depending on severity of the case.

13. Documentation

Complete documentation is required to support system setup, operation and maintenance. The documentation shall include following:

a) Procedures for system setup and use with regards to all features. Documented procedures regarding routine maintenance including use of system diagnostics.

b) Details of hardware/software and as built system.

c) Original copy of licenses in the name of the owner.

Other than the above documents to be submitted at the time of initial implementation the following mandatory documentations should be maintained during the entire period off contract.

a) Weekly, Monthly & Quarterly report on system performance, vulnerability, intrusion, APTs detected with IP address / MAC address of the affected systems, Source & destination IP / Location of the malware etc. detected and other relevant information.

b) Each weekly, monthly & quarterly report should be backed by suitable Incident management report tabulating vulnerabilities & action taken thereof towards correction & corrective action.

c) Documentation towards Patch Management, AV Management, Change Management & other relevant records required for compliance with ISMS standard.

The lists of documents indicated above are among the mandatory records to be generated. However, any other relevant information envisaged for better monitoring & improvement of the system may be adhered to. All documentation shall be delivered in both electronic format (e.g. PDF, MS WORD, Hypertext, etc.) on CDs/DVDs/USB drive, and in hardcopy format. Sufficient on-line, documentation, such as help screens, user guidance messages, context-sensitive help information links, etc., shall be included with the system to minimize the need for users to consult the hardcopy documentation.

----- End of Section-V (TS) ---

पावर सिस्टम ऑपरेशन कॉरपोरेशन लिमिटेड

POWER SYSTEM OPERATION CORPORATION LIMITED

पूर्वी क्षेत्रीय भार प्रेषण केन्द्र

Eastern Regional Load Despatch Centre

14 Golf Club Road, Tollygunge, Kolkata 700033

FORMS & FORMATS (FORMS)

For

IMPLEMENTATION OF MANAGED IT SYSTEM SECURITY SERVICE

And

NETWORK THREAT MONITORING, DETECTION AND RESOLUTION SERVICES

At ERLDC

SECTION - VI

DOC Reference No. : ***ERLDC/C&M/1119/Antivirus etc/2016***	Issue Date: **February 26, 2016**

1. PERFORMANCE SECURITY FORM

Ref. No._____ Dated_____

Power System Operation Corporation Limited,
Eastern Regional Load Despatch Centre
14, Golf Club Road, Tollygunge,
Kolkata – 700 033

WHEREAS _____ Name of Contractor _____ hereinafter called "the Contractor" which expression shall unless repugnant to the context or meaning thereof, include its successors, administrators and assigns has undertaken, in pursuance of Contract No. _____ dated _____ 20 ___ to execute the works (Description of work) hereinafter called "the Contract".

AND WHEREAS it has been stipulated by you in the said Contract that the Contractor shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with the Contractor's performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the Contractor a Guarantee;

THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Contractor, up to a total of _____ (Amount of the Guarantee in Words and Figures) and we undertake to pay you, upon your first written demand declaring the Contractor to be in default under the Contract and without cavil or argument any sum or sums within the limits of _____ (Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the _____ day of _____ 20 _____

Signature and Seal of the Guarantors
with Power of Attorney Number

_____

_____

_____

Date: _____

Address: _____

NOTE:

1. The stamp papers of appropriate value shall be purchased in the name of bank that issues the 'Bank Guarantee'.

2. Performance Security is to be provided by the successful Bidder, as per proforma specified hereinabove, in the form of a bank guarantee from:

   (i) a Public Sector Banks or;

   (ii) Scheduled Indian Banks (*)

   Having paid-up capital (net of any accumulated losses) of Rs. 100 Crores or above

   OR

   (iii) any foreign bank or subsidiary of a foreign bank with overall international corporate rating or Rating of long term debt not less than A(-) (A minus) or equivalent by reputed rating agency. Further, bank guarantee from a foreign bank or subsidiary of a foreign bank should be confirmed by either its correspondent bank located in the country of the Purchaser which should be acceptable to the Purchaser or a Public Sector Bank in the country of Purchaser

   (*) The latest annual report of the bank should support compliance of Capital Adequacy Ratio requirement.

2. FORM OF EXTENSION OF BANK GUARANTEE

Ref. No._____ Dated_____

Power System Operation Corporation Limited,
Eastern Regional Load Despatch Centre
14, Golf Club Road, Tollygumge,
Kolkata – 700 033

Dear Sirs,

Sub: Extension of Bank Guarantee No._____ for _____(*specify currency and amount*) favouring yourselves expiring on _____ on account of M/s _____ in respect of Contract No. _____ dated _____ (hereinafter called original Bank Guarantee).

At the request of M/s. _____ We _____ Bank branch office at _____ having its Head Office at _____ do hereby extend our liability under the above mentioned Guarantee No. _____ Dated _____ for a further period of _____ Years/Months from _____ to expire on _____ Except as provided above, all other terms and conditions of the original Bank Guarantee No. _____dated _____ shall remain unaltered and binding.

Please treat this as an integral part of the original Guarantee to which it would be attached.

Yours Faithfully,

For _____
Manager/Agent/Accountant

Power of Attorney No. _____

Dated _____

SEAL OF BANK

NOTE : The non-judicial stamp paper of appropriate value shall be purchased in the name of the Bank who has issued the Bank Guarantee.

3. PROFORMA FOR APPLICATION FOR PAYMENT

Project	:		
Equipment package	:	Date	:
Name of Contractor	:	Contract No.	:
Contract Value	:	Contract Name	:
Unit reference	:	Application Serial number	:

To
Power System Operation Corporation Limited

Dear Sir,

APPLICATION FOR PAYMENT

Pursuant to the above referred Contract Dated _____ the undersigned hereby applies for payment of the sum of _____ (*specify amount and currency in which claim is made*).

2. The above amount is on account of : (*check whichever applicable*)

   as detailed in the attached schedule(s) which form an integral part of this application.

3. The payment claimed is as per item(s) No(s) of the payment schedule annexed to the above mentioned Contract.

4. The application consists of this page, a summary of claim statement (Schedule**) and the following signed schedule.

   1. _____

   2. _____

   The following documents are also enclosed.

   1. _____

   2. _____

Signature of Contractor/
Authorised Signatory

* Application for payment will be made to 'Engineer-in-Charge' as to be designated for this purpose at the time of award of the Contract.

4. **Details of Electronic Payments**

Name of the Company / Firm / Individual in whose favour payment is to be released.	
Status of Company / others.	
Permanent Account No.	
Service Tax No.	
Address with Pin Code & State	
Correspondence Address	
Telephone No.	
Mobile No.	
Contact Person	
Bank details for electronic payment.	
Name of the Bank	
Address of the Bank	
Account No.	
RTGS No.	
Type of Account	
Branch Code	
9 digit MICR code printed at bottom in meddle next to Cheque No.	

I hereby declare that above information required for electronic payment are correct and true and I agree that the payment on account of my bills be made in the above account maintained in the above mentioned bank.

N.B. A Cancelled Cheque of the Bank is enclosed.

Signature of the Bidder with date :

Signature of the Bidder with date

Name ::

5. **Declaration regarding Social Accountability**

Bidder's Name and Address:

To: Eastern Regional Load Despatch Centre
Power System Operation Corporation Limited,
14 Golf Club Road, Tollygunge,
Kolkata 700033

Dear Sir,

We conform that we stand committed to comply to all requirements of Social Accountability Standards i.e., SA8000 (latest Standard available at www.sa-intl.org) and maintain the necessary records.

Date:.....

Place:.....

(Signature).....

(Printed Name).....…

(Designation).....….....…

(Common Seal)…….…….....

6. **INTEGRITY PACT**

Between

Power System Operation Corporation Limited
(A wholly owned subsidiary of Power Grid Corporation of India Limited)
having its Registered Office at B-9, Qutab Institutional Area, Katwaria Sarai,
New Delhi – 110 016

hereinafter referred to as

"POSOCO",

and

_____

[Insert the name of the Sole Bidder/Lead Partner of Joint Venture]

having its Registered Office at _____
(Insert full Address)

_____

Hereinafter referred to as

"The Bidder/Contractor"

Preamble

POSOCO intends to award, under laid-down organizational procedures, contract(s) for _____ *[Insert the name of the package]*

Package and Specification Number _____ *[Insert Specification Number of the package]* POSOCO values full compliance with all relevant laws and regulations, and the principles of economical use of resources, and of fairness and transparency in its relations with its Bidders/ Contractors.

In order to achieve these goals, POSOCO and the above named Bidder/Contractor enter into this agreement called '**Integrity Pact**' which will form a part of the bid.

It is hereby agreed by and between the parties as under:

Section I - Commitments of POSOCO

(1) POSOCO commits itself to take all measures necessary to prevent corruption and to observe the following principles:

a) No employee of POSOCO, personally or through family members, will in connection with the tender, or the execution of the contract, demand, take a promise for or accept, for him/herself or third person, any material or other benefit which he/she is not legally entitled to.

b) POSOCO will, during the tender process treat all Bidder(s) with equity and fairness.

POSOCO will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/ additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

(c) POSOCO will exclude from evaluation of Bids its such employee(s) who has any personnel interest in the Companies/Agencies participating in the Bidding/Tendering process

(2) If CEO obtains information on the conduct of any employee of POSOCO which is a criminal offence under the relevant Anti-Corruption Laws of India, or if there be a substantive suspicion in this regard, he will inform its Chief Vigilance Officer and in addition can initiate disciplinary actions under its Rules.

Section II - Commitments of the Bidder/Contractor

(1) The Bidder/Contractor commits himself to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution:

a) The Bidder/Contractor will not, directly or through any other person or firm, offer, promise or give to POSOCO, or to any of POSOCO's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange an advantage during the tender process or the execution of the contract.

b) The Bidder/Contractor will not enter into any illegal agreement or understanding, whether formal or informal with other Bidders/Contractors. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or actions to restrict competitiveness or to introduce cartelization in the bidding process.

c) The Bidder/Contractor will not commit any criminal offence under the relevant Anti-corruption Laws of India; further, the Bidder/Contractor will not use for illegitimate purposes or for purposes of restrictive competition or personal gain, or pass on to others, any information provided by POSOCO as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d) The Bidder/Contractor of foreign origin shall disclose the name and address of the Agents/representatives in India, if any, involved directly or indirectly in the Bidding. Similarly, the Bidder/Contractor of Indian Nationality shall furnish the name and address of the foreign principals, if any, involved directly or indirectly in the Bidding.

e) The Bidder/Contractor will, when presenting his bid, disclose any and all payments he has made, or committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract and/or with the execution of the contract.

f) The Bidder/Contractor will not misrepresent facts or furnish false/forged documents/informations in order to influence the bidding process or the execution of the contract to the detriment of POSOCO.

(2) The Bidder/Contractor will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section III- Disqualification from tender process and exclusion from future contracts

(1) If the Bidder, before contract award, has committed a serious transgression through a violation of Section II or in any other form such as to put his reliability or credibility as Bidder into

question, POSOCO may disqualify the Bidder from the tender process or terminate the contract, if already signed, for such reason.

(2) If the Bidder/Contractor has committed a serious transgression through a violation of Section II such as to put his reliability or credibility into question, POSOCO may after following due procedures also exclude the Bidder/Contractor from future contract award processes. The imposition and duration of the exclusion will be determined by the severity of the transgression. The severity will be determined by the circumstances of the case, in particular the number of transgressions, the position of the transgressors within the company hierarchy of the Bidder/Contractor and the amount of the damage. The exclusion will be imposed for a minimum of 12 months and maximum of 3 years.

(3) If the Bidder/Contractor can prove that he has restored/recouped the damage caused by him and has installed a suitable corruption prevention system, POSOCO may revoke the exclusion prematurely.

Section IV - Liability for violation of Integrity Pact

(1) If POSOCO has disqualified the Bidder from the tender process prior to the award under Section III, POSOCO may forfeit the Bid Guarantee under the Bid.

(2) If POSOCO has terminated the contract under Section III, POSOCO may forfeit the Contract Performance Guarantee of this contract besides resorting to other remedies under the contract.

Section V- Previous Transgression

(1) The Bidder shall declare in his Bid that no previous transgressions occurred in the last 3 years with any other Public Sector Undertaking or Government Department that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

Section VI - Equal treatment to all Bidders/Contractors

(1) POSOCO will enter into agreements with identical conditions as this one with all Bidders.

(2) POSOCO will disqualify from the tender process any bidder who does not sign this Pact or violate its provisions.

Section VII - Punitive Action against violating Bidders/Contractors

If POSOCO obtains knowledge of conduct of a Bidder or a Contractor or his subcontractor or of an employee or a representative or an associate of a Bidder or Contractor or his Subcontractor which constitutes corruption, or if POSOCO has substantive suspicion in this regard, POSOCO will inform the Chief Vigilance Officer (CVO).

(*)**Section VIII - Independent External Monitor/Monitors**

(1) POSOCO/POWERGRID has appointed a panel of Independent External Monitors (IEMs) for this Pact with the approval of Central Vigilance Commission (CVC), Government of India, out of which one of the IEMs has been indicated in the NIT/IFB.

(2) The IEM is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement. He has right of access to all project documentation. The IEM may examine any complaint received by him and submit a report to CEO, POSOCO, at the earliest. He may also submit a report directly to the CVO and the CVC, in case of suspicion of serious irregularities attracting the provisions of the PC Act. However, for ensuring the desired transparency and objectivity in dealing with the complaints arising out

of any tendering process, the matter shall be referred to the full panel of IEMs, who would examine the records, conduct the investigations and submit report to CEO, POSOCO, giving joint findings.

(3) The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the CEO, POSOCO.

(4) The Bidder(s)/Contractor(s) accepts that the IEM has the right to access without restriction to all documentation of POSOCO related to this contract including that provided by the Contractor/Bidder. The Bidder/Contractor will also grant the IEM, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his documentation. The same is applicable to Subcontractors. The IEM is under contractual obligation to treat the information and documents of the Bidder(s)/Contractor(s)/Subcontractor(s) with confidentiality.

(5) POSOCO will provide to the IEM information as sought by him which could have an impact on the contractual relations between POSOCO and the Bidder/Contractor related to this contract.

(6) As soon as the IEM notices, or believes to notice, a violation of this agreement, he will so inform the CEO, POSOCO and request the CEO, POSOCO to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit non-binding recommendations. Beyond this, the IEM has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action. However, the IEM shall give an opportunity to POSOCO and the Bidder/Contractor, as deemed fit, to present its case before making its recommendations to POSOCO.

(7) The IEM will submit a written report to the CEO, POSOCO within 8 to 10 weeks from the date of reference or intimation to him by POSOCO and, should the occasion arise, submit proposals for correcting problematic situations.

(8) If the IEM has reported to the CEO, POSOCO, a substantiated suspicion of an offence under relevant Anti-Corruption Laws of India, and the CEO, POSOCO has not, within the reasonable time taken visible action to proceed against such offence or reported it to the CVO, the Monitor may also transmit this information directly to the CVC, Government of India.

(9) The word '**IEM**' would include both singular and plural.

(*) This Section shall be applicable for only those packages wherein the IEMs have been identified in Section – I : Invitation for Bids and/or Clause ITB 9.3 in Section – III: Bid Data Sheets of Conditions of Contract, Volume-I of the Bidding Documents.

Section IX - Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor after the closure of the contract and for all other Bidder's six month after the contract has been awarded.

Section X - Other Provisions

(1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the establishment of POSOCO. The Arbitration clause provided in the main tender document / contract shall not be applicable for any issue / dispute arising under Integrity Pact.

(2) Changes and supplements as well as termination notices need to be made in writing.

(3) If the Contractor is a partnership firm or a consortium or Joint Venture, this agreement must be signed by all partners, consortium members and Joint Venture partners.

(4) Nothing in this agreement shall affect the rights of the parties available under the General Conditions of Contract (GCC) and Special Conditions of Contract (SCC).

(5) Views expressed or suggestions/submissions made by the parties and the recommendations of the ***CVO/***IEM# in respect of the violation of this agreement, shall not be relied on or introduced as evidence in the arbitral or judicial proceedings (arising out of the arbitral proceedings) by the parties in connection with the disputes/differences arising out of the subject contract.

CVO shall be applicable for packages wherein IEM are not identified in Section IFB/BDS of Condition of Contract, Volume-I. IEM shall be applicable for packages wherein IEM are identified in Section IFB/BDS of Condition of Contract, Volume-I.

(6) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(Signature) _____ **(For & On behalf of POSOCO)**	(Signature) _____ **(For & On behalf of Bidder/ Partner(s) of Joint Venture/ Contractor)**
(Office Seal)	(Office Seal)
Name:_____	Name:_____
Designation:_____	Designation:_____
Witness 1 :_____	Witness 1 :_____
(Name & Address) _____	(Name & Address) _____
_____	_____
Witness 2 :_____	Witness 2 :_____
(Name & Address) _____	(Name & Address) _____
_____	_____

1. Bid-Data Sheet for Implementation of Managed IT System Security Service

1.1. Key Features

S/N	Functional Features	Yes / No	Deviation taken (if Any)
1	Indicate whether dedicated Anti-APT hardware Device provided?		
2	Indicate whether proposed hardware device is integrated within the ERLDC LAN		
3	Indicate whether proposed hardware device is capable of monitoring both internal and external threats		
4	Indicate whether proposed security management service includes ERLDC LAN boundary and its connectivity with other LAN / WAN Zones and public domains		
5	Indicate whether the Anti-APT Hardware & associated service provides advanced threat protection with 360-degree network monitoring of all traffic to detect all aspects of a targeted attack		
6	Indicate whether the Anti-APT device has Integrated Specialized detection engines and custom sandboxes to identify and analyse malware, command-and-control (C&C) communications, and evasive attacker activities that are invisible to standard security defences		
7	Indicate whether other Key features as indicated in sl. 1.2 of TS is complied (specify deviation if any)		
8	Indicate whether separate Client-Server 100 Users License AV suite considered		
9	Indicate whether the AVA suite is of same OEM as that of the Anti-APT device		
10	Indicate whether Tender Specific MAF submitted		
11	Indicate whether the vendor is authorised partner of the OEM		
12	Indicate whether scope covers 3 years AMC & SIEM support		
13	Indicate whether all software is licensed for minimum 3 years including free support & upgrade		
14	Indicate whether the product offered is leading solution for desired scope (Provide necessary documentary proof such as NSS Lab recommendation, Gartner review etc.		

1.2. Bid Data Sheet for Anti-APT Hardware

S/N	Functional Features	Yes / No	Deviation taken (if Any)
A	**Make**		
B	**Model**		
1.0	***General Specs***		
1.1a	Whether proposed solution is able to inspect the multi-protocol sessions to detect and flag the suspicious activity?		
1.1b	Whether such detection includes suspicious file downloads through the web, the suspicious mail attachment and internal infections?		
1.2	Whether proposed solution supports the native CEF, LEEF format for SIEM log integration?		
1.3a	Whether proposed solution is able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects?		
1.4	Whether proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network?		
1.5	Whether upon detection of the threat, the proposed solution is able to perform behaviour analysis for advance detection?		
1.6	Whether proposed solution has event detection capabilities that include malware type, severity, source and destination of attack?		
1.7a	Whether the proposed solution provides risk based alerts or logs?		
1.7b	Whether such logs provide facility to prioritize remediation effort?		
1.8	Whether proposed solution is designed to be deployed on premise along with on premise sandboxing capability?		
1.9	Indicate storage capacity available with the proposed solution to store payload of the detected threats.		

S/N	Functional Features	Yes / No	Deviation taken (if Any)
1.10	Whether proposed solution has ability to interrupt malicious communication?		
1.11a	Indicate number of concurrent users supported.		
1.11b	Indicate Bandwidth supported.		
1.12	Whether proposed solution is able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment?		
1.13	Provide URL/Information regarding OEMs own threat intelligence portal for further investigation, understanding and remediation of an attack.		
1.14	Whether proposed solution is able to support out-of-band detection?		
1.15	Whether the proposed solution is able to detect (lateral moments) movement of the attacker and the attacks within organization's network?		
1.16	Indicate whether the proposed solution has any port based limitation? If NO indicate deviations thereof.		
1.17	Indicate whether all standard protocols as required / defined in TS are supported for inspection? Specify Deviation		
1.18	Whether the proposed solution supports to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance?		
1.19	How many network segments on a single appliance is supported (specify)?		
1.20	Whether the proposed solution is able to detect communications to known command and control centres?		
1.21	Whether the proposed solution is able to detect reputation of url being accessed?		
1.22	Indicate whether the severity and stage of each attack is identifiable separately by the proposed solution?		
1.23	Whether the proposed solution has built in capabilities to add exceptions for detections?		

S/N	Functional Features	Yes / No	Deviation taken (if Any)
1.24	Whether the proposed solution has capabilities to configure files, IP, URLs and Domains to Black list or white list?		
1.26	Whether the proposed solution has a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis?		
1.27	Whether the proposed solution provides correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal?		
1.28	Whether the proposed solution is able to contain, remediate and quarantine the threats on the all the endpoints of the organization		
2.0	***Malware Analysis***		
2.1	Whether the proposed solution has multiple built-in virtual execution environments within single appliance?		
2.2	Whether the proposed solution is able to provide customizable sandbox?		
2.3	Indicate whether Sandbox supports multiple operating systems and for both 32-bits and 64-bits OS? Specify OS not supported.		
2.4	Indicate Maximum File size supported for analysis (specify in MB).		
2.5	Indicate whether Sandbox has the ability to simulate the entire threat behaviour (honeynet and honeypot framework supported – yes/no)		
2.6	Whether the proposed solution has grey ware detection capabilities?		
2.7	Provide information regarding web service interface/API provided to customize their system integration.		
2.8	Whether the proposed solution has capability to scale out the detection when the bandwidth increases?		
2.9	Indicate whether multiple file format analysis as indicated in TS complied.		

S/N	Functional Features	Yes / No	Deviation taken (if Any)
2.10	Whether the proposed solution has built-in document vulnerabilities detection engine?		
2.11	Whether the proposed solution provides the capability for further investigation of exportable network packet files and encrypted suspicious files?		
2.12	Whether the proposed solution has the capability to perform tracking and analysis of virus downloads and suspicious files?		
2.13	Whether the proposed solution has capabilities to scan inside password protected Archives		
2.14	Whether the proposed solution has capabilities to configure files, IP, URLs and Domains to Black list or white list		
2.15	Whether the proposed solution has capability to include User-defined and context-derived passwords for protected archives		
2.16	Whether the proposed solution has capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.		
2.17	Whether the proposed solution is able to detect known malwares before sending suspicious files to Sandbox for analysis		
2.18	Whether the proposed solution is able to correlate local APT attacks with Global historical APT attacks.		
2.19	Indicate the throughput supported (specify in GBPS)		
2.20	What is the usable storage available (specify in GB)		
2.21	How many 10/100/1000 Ethernet Interfaces provided (specify)		
3.0	***Report***		
3.1	Whether the proposed solution has an intuitive Dashboard that offers real time threat visibility and attack characteristics		

S/N	Functional Features	Yes / No	Deviation taken (if Any)
3.2	Indicate Formats of reports available (specify file format)		
3.3	Whether the proposed solution is able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time)		
3.4	Whether the proposed solution supports logging of important parameters in the report like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attacks sessions.		
3.5	Whether the proposed solution has dashboard capable of displaying correlated graphical data that is based on link-graph, geo-map, chart, tree-map/pivot table.		
3.6	Whether the proposed solution provides in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.		
3.7	Whether the proposed solution has capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.		
3.8	Whether the proposed solution is able to generate out of box reports to highlight Infections, C&C behaviour, Lateral Moment, Asset and data discovery and Exfiltration		
4.0	***Authentication Administration and Configuration Requirement***		
4.1	Whether the proposed solution supports Local Password authentication schemes		
4.2	Whether the proposed solution supports Remote administration using SSH/HTTPS		
4.3	Whether the proposed solution supports CLI, GUI/Web based Administration Console.		

The Data-sheet should be filled in details, clearly indicating deviations (if any). Necessary documentary proof in form of brochures / datasheet highlighting the compliance parameters may be attached. Bids with ambiguously filled Bid-Data sheet are liable for rejection.

1.3. Bid Data Sheet for Anti-virus / Anti-Spam / Anti-Malware Security Suite

3 (three) years 100 (one Hundred) Users License AV Protection Suite of reputed make (preferably same OEM as that of the Anti-APT solution proposed) should be provided and suitably installed at designated Desktop / Laptop & Servers as per satisfaction of the consignee representative. Manageability of the AV suite for its 3 (three) year life shall be within the scope of this contract.

A detailed data-sheet indicating preferred features of the AV Suite is tabulated below:

S/N	Functional Features	Yes / No	Deviation taken (if Any)
A	**Make**		
B	**Model**		
C	**No. of Users**		
D	***Antivirus Protection and Other features***		
1	Whether offer client/server based security implementation. by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.		
2	Whether enterprise level protection from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks provided.		
3	Whether is able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.		
4	Whether capabilities for detecting and removing rootkits available		
5	Whether Real-time spyware/grayware scanning for file system to prevent or stop spyware execution provided		
6	Whether has capabilities to restore spyware/grayware if the spyware/grayware is deemed safe		
7	Whether cleans computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process		
8	*Whether to address the threats and nuisances posed by Trojans, the solution is able to do the following:*		
8.1	Terminating all known virus processes and threads in memory		
8.2	Repairing the registry		
8.3	Deleting any drop files created by viruses		
8.4	Removing any Microsoft Windows services created by viruses		

S/N	Functional Features	Yes / No	Deviation taken (if Any)
8.5	Restoring all files damaged by viruses		
8.6	Includes Clean-up for Spyware, Adware etc.		
9	Whether capable of cleaning viruses/malware even without the availability of virus clean-up components?		
10	Whether provides Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients in case there is an outbreak		
11	Whether perform Behaviour Monitoring as indicated in the TS		
12	Whether provides feature to allow or prevent users from changing settings or unloading/uninstalling the software		
13	Whether provides CPU usage performance control during scanning as per TS		
14	Whether has Integrated spyware protection and clean-up		
15	Whether has the capability to assign a client the privilege to act as a update agent for rest of the agents in the network		
16	Whether is able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)		
17	Whether safeguards endpoint mail boxes by scanning incoming POP3 email and Outlook folders for Threats		
18	Whether able to scan only those file types which are potential virus carriers (based on true file type)		
19	Whether is able to detect files packed using real-time compression algorithms as executable files.		
20	Whether is able to manage both SaaS and on premise solution from the single management console		
21	Whether is able to scan Object Linking and Embedding (OLE) File		
E	***Manageability and integration***		
1	Whether provides Comprehensive Support for Network Admission Control		
2	*Whether is able to deploy the Client software using the following mechanisms:*		
2.1	Client Packager (Executable & Microsoft Installer (MSI) Package Format)		
2.2	Web install page		
2.3	Login Script Setup		
2.4	Remote installation		

S/N	Functional Features	Yes / No	Deviation taken (if Any)
2.5	From a client disk image		
2.6	MS Systems Management Server (SMS)		
3	Whether provides a secure Web-based management console to give administrators transparent access to all clients and servers on the network		
4	Whether management server is able to download updates from different source if required, which could be the vendor's update server, any other server or a UNC path		
5	If the update from the Management server fails, whether the security clients with the privilege is able to get updated directly from the vendor's server		
6	Whether network traffic generated is reduced when downloading the latest pattern by downloading only incremental patterns		
7	Whether has the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console		
8	*Whether has role based administration with active directory integration having following features*		
8.1	To create custom role type		
8.2	To add user to a predefined role or to a custom role		
8.3	Integration with the Active directory		
8.4	Support grouping of clients into domains for easier administration		
9	Whether establishes separate configuration for internally versus externally located machines		
10	Whether offer centrally managed Client Firewall and IDS		
F	***Platform Support***		
1	Indicate whether all OS as mentioned in the TS supported (specify deviation – if any)		
2	Whether supports Intel x64 processor & AMD x64 processor		
3	Whether supports wireless devices such as Palm, Pocket PC, and EPOC at no extra cost		
G	***Notification, Reporting and logging***		
1	Whether is able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via E-mail, Pager, SNMP trap or Windows NT Event log		

S/N	Functional Features	Yes / No	Deviation taken (if Any)
2	Whether is able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack		
3	Whether offers customizable & standard notifications via - SMTP, SNMP, Pager, NT Event Log (No additional agent)		
4	Whether Protect Data at rest, in use, and in Motion		
5	Whether is integrated with Gateway URL Filtering/Proxy Server and Endpoint Antivirus with no addition agent deployment		
6	Whether detects and reacts to improper data use based on keywords, regular expressions and file attributes		
7	Whether is able to restrict the use of USB drives, CD/DVD writers, and other removable media		
8	Whether offers granular device control, including the ability to create specific rules based on make and serial number of the device		
9	Whether tracks and documents sensitive data flowing through network egress points		
10	Whether automates response to policy violations with options to log, bypass, block, encrypt, alert, modify, quarantine, or delete data		

The Data-sheet should be filled in details, clearly indicating deviations (if any). Necessary documentary proof in form of brochures / datasheet highlighting the compliance parameters may be attached. Bids with ambiguously filled Bid-Data sheet are liable for rejection.

1.4. Bid Data Sheet for Security Incident Event management Service

S/N	Functional Features	Yes / No	Deviation taken (if Any)
1	Indicate whether generation of periodic report as per requirement of TS has been considered in the scope. (A copy of sample report may be attached for better understanding)		
2	Indicate the parameters which will be monitored & reflected in the report (specify as many as possible)		
3	Indicate whether action towards all remedial measures required as per finding of the report has been considered within the scope of the contract.		

S/N	Functional Features	Yes / No	Deviation taken (if Any)
4	Indicate whether necessary documentation towards corrections & corrective actions considered in the scope		
5	Indicate whether periodic VAPT and measures for Preventive action considered in the scope (specify VAPT periodicity)		
6	Indicate whether Information asset Risk Assessment & Risk Treatment considered in the scope (specify periodicity)		
7	Provide detailed plan for preparation & scope during Third Party Audit		
8	Indicate the Manpower deployment plan for SIEM & Remedial actions (specify periodicity of visit, Man-days considered etc. in details)		
9	Indicate qualification & experience of Front Level Security Engineer to be deputed (enclose CV)		
10	Indicate qualification & experience of Expert Level Security Engineer to be deputed (enclose CV)		
11	Indicate qualification & experience of Delivery Head to be deputed (enclose CV)		

2. Bidding Schedule

S/N	Item Description	Quantity	Rate	Amount
A	**Hardware & Software Product Portion** *(To be Paid after successful Installation & Commissioning as per Part A of Payment Terms)*			
1	Anti-Advanced Persistent Threat Hardware	1 Set		
2	Anti-Advanced Persistent Threat Software (In-built with Hardware above)	1 Set		
3	100 Users License of AV/Anti-Malware Suite for 3 years (including media if any)	100 Users pack		
Sub Total (A) – excluding taxes				
Taxes & Duties on A above				
Sub Total (A) – including taxes				
B	**Support, Subscription & Service Portion** *(To be Paid on yearly basis after completion of the period for 3 years in 3 equal instalments)*			
1	Software subscription & support for Anti-APT Software	3 years support		
2	AMC Charges for Anti-APT Hardware after completion of 1 year warranty	2 years AMC		
3	SIEM Service including deputation of Manpower for monitoring, remediation, documentation and other associated service	3 years SIEM		
Sub Total (B) – excluding taxes				
Taxes & Duties on B above				
Sub Total (B) – including taxes				
Total (A+B) – including taxes				
C	**Any other Charges (please indicate details)**			
1	(indicate details including taxes)			
Grand Total (A + B + C) – including taxes				

Note:

1. POSOCO, ERLDC will not issue "C" Form.
2. The ratio of A (excluding taxes) : B (excluding taxes) should not be greater than 65:35. i.e. A (excluding taxes) should not be by any means greater than 65% of the Total cost of the contract (excluding taxes). Bids received with deviation in this connection or bids received with cost of A greater than 65% of the total cost of contract is liable for rejection subject to modification of payment terms to accommodate such ratio.

पावर सिस्टम ऑपरेशन कॉरपोरेशन लिमिटेड

(पावरग्रिड की पूर्ण स्बामित्ब प्राप्त सहायक कंपनी)

POWER SYSTEM OPERATION CORPORATION LIMITED

(A wholly owned subsidiary company of POWERGRID)

पूर्वी क्षेत्रीय भार प्रेषण केन्द्र

Eastern Regional Load Despatch Centre

14 Golf Club Road, Tollygunge, Kolkata 700033