Corrigendum - 3

01. Consolidated replies to the Technical Pre-Bid Queries received post Pre-bid meeting

Tender No	TPSODL/OT/2021-22/004
Package Name	SCADA and ADMS System for TP Southern Odisha Distribution Limited

Sr. No.	Detailed Reference to Tata Power Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
1	2	3	4	5
1	(Page- 38) 3.6.8	A contract for upgrades to be performed by the software supplier. This contract shall include the software upgrade service described above, plus on-site installation service to be provided by the software supplier	Is software Upgrade in the scope of this contract? If so, we request TPSODL to kindly exclude the same as SCADA software upgrade may involve a major re-implementation work.	As per RFP.
2	(Page- 41)4.6 Sl. No 1 a. - Tech Evaluation table	Number of SCADA/ADMS project successfully completed in last 8 years. as meeting the Technical Requirements	As we are considering Experience in Evaluation Criteria, We request TPSODL to kindly exclude the period of 8 years	As per RFP
3	(Page- 46)1.3 - Scope of work	Power system network analysis	What functions should Power System Network Analysis include? TPSODL may please clarify	EMS application requirement is not in scope however Power flow analysis at Distribution points is considered
4	(Page- 51) 2.1.4 Design and Coding Standards for SCADA/ADMS applications, Pt a	Expansion/ scalability: software shall be dimensioned to accommodate the ultimate size of SCADA/ADMS system envisaged	What is the tag count of the current SCADA System at TPSODL. What is the scalability expected?	Refer Appendix-C
5	(Page- 54) 2.1.6.6 Distributed Backup and Archiving	Once initiated, the distributed backup and archiving services shall automatically back up all information needed to recover from failures or data corruption without manual intervention by users, except for replenishment of removable media	We understand tape backup needs to be done. TPSODL may please confirm. If so how many years back up need to be maintanined?	5 years back up needs to be maintained.
6	(Page- 59) 2.2.3.4 Initial Database Generation	The Contractor shall arrange the required software tool to acquire the initial data from the existing control centre at his own cost. The owner shall provide the access to these regional control centres for acquiring the required data.	In what form will the initial data be available from the existing CC. TPSODL may please clarify.	existing DCU/RTU/FRTU will be reporting over IEC 60870-5-104 to existing local DMS. The migration will be performed by Bidder .
7	(Page- 71) 2.7.1.2 SCADA/ADMS from GIS Interface	The SCADA/ADMS solution shall have a CIM compliant interface for network model exchange as a standard integration mechanism with GIS. In case the solution is not CIM compliant, necessary adapter has to be provided.	What is the and version of the existing GIS at TPSODL?	As communicated during pre-bid meeting on 2.6.21, GIS server system is under finalization.
8	(Page- 72) 2.7.1.3 SCADA/ADMS from/to CIS (SAP ISU) Interface	The SCADA/ADMS will need to receive trouble calls from the CIS on an interactive basis. This includes all IVR calls received by the CIS.	We understand that Integration middleware is already implemented in TPSODL. TPSODL may please confirm. If so what is the middleware that is implemented?	As communicated during pre-bid meeting on 2.6.21, CIS will be part of proposed system only. SAP-PI is already in place in TPSODL.
9	(Page- 72) 2.7.1.4 SCADA/ADMS to IVR Interface	There is no direct interface from the SCADA/ADMS to the IVR, All information routed is through fluent grid -CIS. It is intended that the IVR to fluent grid CIS interface will capture necessary information to create a trouble ticket that can in-turn pass to the SCADA/ADMS.	We understand that the Fluent Grid CIS is already integrated to the SAP ISU. TPSODL may please confirm/clarify.	As per RFP.
10	(Page- 72) 2.7.1.6 SCADA/ADMS from AMI Interface Table 2.6 -	There will be interfacing available in SCADA/ADMS to connect with TPSODL’ AMI/ Meter management system.	We understand that the MDMS shall pass on the outage/Event information to the OMS system.Please clarify the use case of integrating SCADA/ADMS with the AMI system.	As communicated during pre-bid meeting on 2.6.21, AMI is under finalization
11	(Page- 107) 4.7 Browser-based User Interface	The user interface software shall be based on state-of-the-art web-based technology to present interactive, full-graphics views of system data via LAN, corporate intranet or the internet. The same displays shall be used.	To the best of our knowledge Screens of reputed SCADA products would not be available over the internet as a Web Browser. TPSODL may kindly review the requirement	Shall be as per RFP
12	(Page- 117) 5.2.2.4 Web servers:	Redundant Web servers shall be provided. The third-party interface will be developed from this server. Web server shall support JSON REST API, MQTT inputs for IOT	Why should the Web Server support IoT protocols such as JSON, REST API, MQTT, etc. TPSODL may please clarify.	Shall be as per RFP
13	(Page- 177) 8.2.2 Weather Variables	The weather adaptive forecast shall use actual load data, actual weather data and weather forecast data to calculate a load forecast.	How will the Weather data be received at CC. TPSODL may please clarify.	Provision to be considered by the bidder.
14	(Page- 45) 1st Paragraph		Is there any possibility of addition of substations/RTUs including the existing 257 number of 33/11 kv and 28 number of 132/11 kv.	Shall be considered as per RFP.
15	(Page- 59) 4tth Paragraph		RTU side configuration during integration to SCADA is SI's out of Scope	RTU configuration is in purchaser's scope however shall be completed as per project requirement by the bidder.
16	(Page- 220) 10.4.9 Strom Management		Is there any existing weather forecasting system, Is interface with this system is SI's Scope	No, however interface provision to be considered by the bidder.
17	(Page- 46) Scope of work		Study of existing deployed Micro SCADA and migration along with interfaces planned by TPSODL, please elaborate the quatum of data and type of data	All substations having local DMS shall be migrated.

Sr. No.	Detailed Reference to Tata Power Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
18	(Page- 46) Supply, installation, integration & commissioning of Supervisory Control and Data Acquisition (SCADA) system and Information Storage & Retrieval (ISR) Functions with following features: - Power system network analysis		It is expected to supply ISR system, with Power system N/w analysis, please elaborate the requirement	As communicated during pre-bid meeting on 2.6.21, all functionalities of SCADA/ADMS shall be provided.
19	(Page- 15) Project Start Part-B DMS & OMS (tentative)		Please explain the meaning of tentative	Bidder to take all efforts to meet the schedule for completion of part-A and start on part-B.
20	1.7/c Qualification Requirement/Eligibility Criteria Page no 7	The Bidder shall provide evidence of previous experience in the design, engineering, supply, installation, testing and commissioning of SCADA & ADMS (Supervisory Control and Data Acquisition System & Advance Distribution Management System) in multiple Projects (Maximum 3 nos.) for Power Distribution Systems (11KV or above) in the last eight (8) years.	**Bidder/System Integrator/Authorized representative of OEM/Channel Partne**r shall provide evidence of previous experience in the design, engineering, supply, installation, testing and commissioning of SCADA & ADMS (Supervisory Control and Data Acquisition System & Advance Distribution Management System) in multiple Projects (Maximum 3 nos.) for Power Distribution Systems (11KV or above) in the last eight (8) years.	As per RFP.
21	5.4.2 Control Center WAN page no 118	As per clause no. we understand the CC WAN is in scope of TPSODL.	Please confirm whether the CC WAN cover the RTUs/DCUs to be located at various substations. Also, does the CC WAN cover the three Area Power Control Centres and the links to LDC and external utility? If the Micro SCADA is to be retained in the new architecture, we need to have it's details, like it's location, what all public interfaces it provides, what all RTUs report to it etc. Further,does each RTU/DCU have to have redundant comm link to MCC and BCC?	WAN Communication is in scope of TPSODL. Existing local DMS / Micro SCADA will not be retained.
22	TPSODL/BOM/285	Security system (DMZ) - Layer II switch	No. of port for Layer II switch not mentioned 24 or 28 ports. Can we consider 24 ports for Layer II switch here?	Ok.
23	TPSODL/BOM/285	External Mass storage device (for year online backup)	No. of SAN storage mentioned are 4 but SAN switch quantity is not mentioned. Can we consider 4 SAN switches here?	As per the configuration.
24	TPSODL/TABLE A/12 PANEL/135	PANEL	It is requested to mention quantities of PANEL that will be used in each location Berhampur City (MCC), Jeypore /Sambalpur (BCC), Aska, Bhanjnagar, Rayagada and Jeypore	As per RFP there are two physical locations, one is MCC and other is BCC.The servers are inclusive of Rack and KVM switches as per configuration requirement.
25	TPSODL/TABLE A/12 PANEL/135	PANEL	KVM Switch specification is not mentioned. It is requested to add quantities of KVM Switch.	As per RFP there are two physical locations, one is MCC and other is BCC.The servers are inclusive of Rack and KVM switches as per configuration requirement.
26	TPSODL/TABLE A/12 PANEL/135	PANEL	It is requested to mention quantities KVM switches.	As per RFP there are two physical locations, one is MCC and other is BCC.The servers are inclusive of Rack and KVM switches as per configuration requirement.
27	TPSODL/Tentative BoQ/12.14	NMS Specs	Number of nodes for NMS software mentioned is 10000.However we can calculate the number of nodes and keep 20% spare and provide NMS solution with actual number of required nodes.	Shall be as per revised NMS specs
28	TPSODL/Tentative BoQ/12.14	NMS Specs	We need to consider KVM switch,sliding monitor for NMS systems only.Also please share specs for the same if possible.	As per RFP there are two physical locations, one is MCC and other is BCC.The servers are inclusive of Rack and KVM switches as per configuration requirement.

02. Consolidated replies to the Commercial Pre-Bid Queries received post Pre-bid meeting

Tender No	**TPSODL/OT/2021-22/004**			
Package Name	**SCADA and ADMS System for TP Southern Odisha Distribution Limited**			
1	TPSODL/OT/2021-22/004/GCC/14.2/24	In case of no mention of the guarantee period in standard specifications or SCC Guarantee Period will be 12 Months from the Date of Commissioning or 24 months from the date of delivery of final lot of supplies made, whichever is earlier.	Contradicting with warranty period mentioned in other clauses.	For this cluase Special Conditions for Contract / Scope of Work shall supersued General Conditions of Contract.
2	TPSODL/OT/2021-22/004/GCC/14.3/24	If during the Warranty/ Guarantee period some parts of the supplies are replaced owing to the defects/ damages under the Warranty, the Warranty period for such replaced parts shall be until the expiry of twelve months from the date of such replacement or renewal or until the end of original Guarantee period, whichever is later.	Total warranty period of the system is specified then this clause for the warranty of individual component shall be removed.	As per RFP
3	TPSODL/OT/2021-22/004/GCC/22.0/28	20.0 FORCE MAJEURE	Does not have clause of pandemic in the Force Majeure	Yes, COVID-19 is not a part of GCC / tender documents but in case Central Government declare Covid as Force Majere then we shall consider the same for specific project.

Sr. No.	Detailed Reference to Tata Power Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
4	TPSODL/OT/2021-22/004/GCC/15.0/24	14.0 LIQUIDATED DAMAGES For delay of each week and part thereof from the delivery schedule specified in the contract, 1% of contract value corresponding to undelivered quantity, provided full quantity is supplied within 130% of the original contract time. If full contractual quantity is not delivered within 130% of contract time for delivery, TPSODL has the right to levy LD on the entire contract value, subject to a maximum of 10% of the total contract value.	Statement not understood. Kindly provide more details on this.	In case delay in full / part delivery of services / supply as per scheduled specified in the tender enquiry, LD shall levy 1% for each week. If full contractual quantity is not delivered within 130% of contract time for delivery, TPSODL has the right to levy LD on the entire contract value, subject to a maximum of 10% of the total contract value.
5	TPSODL/OT/2021-22/004/GCC/6.0/13	PBG	5% advance on submission of 5% ABG & 10% CPBG. Ideally 5% advance should have been released against 5% ABG. 5%/10% PBG can be submitted at the time of claiming the last payment amount. Last milestone payment is 5% then why PBG of 10% is needed.	1. Bidder shall submit the ABG of 5% of Contract Value. BA shall submit the ABG within 15 days. This shall remain valid till the Guarantee period plus one month. 5% advance shall be paid by TPSODL. 2. CPBG of 5% of Contract Value .BA shall subit the CPBG within 30 days from the date of issue of work order. This shall remain valid till the Guarantee period plus one month
6	TPSODL/OT/2021-22/004/GCC/6.0/13	Payment Terms	Supply of SCADA and ADMS system cannot be staggered. The entire system has to be shipped and installed together after FAT. Howeever commisioning and integration activities of SCADA and ADMS can be staggered. Hence in this regard we request you to amend the payment terms as below. MS-1(a): unchanged MS-1(b): unchanged MS-2: unchanged MS-3: 50% of total contract value on receipt of material at site MS-4: 5% on installation and commisioning of SCADA MS-5: 5% on installation and commisioning of ADMS including integrations MS-6: 5% on SAT of complete system MS-7: 5% on operational acceptance of complete system	As per RFP
7	TPSODL/OT/2021-22/004/3.3/32	Phased Deliveries The SCADA/ADMS will be delivered in at least two Part. Deliverables of each Part/phase are described in. The requirements of this maintenance program shall be applied to each phase as follows: 1) SCADA System – The SCADA shall undergo factory, site, and availability tests. 2) ADMS Applications – GIS CIM based network and The SCADA/DMS/OMS Applications shall undergo factory, site, and availability tests.	Please clarify the reason for phased deliveries.	For focused and better implementation of project.
8		Bid Extension	Request you to extend the bid submission date by 6 weeks	Due date shall not extend
9	TPSODL/OT/2021-22/004 / 7.4 / 15	The complete solution including hardware/ software shall be under comprehensive on-site warranty for a period of 60 months from the date of project completion as mentioned in Scope of Work in Annexure II.	IT should be from the date of supply at site	As per RFP
10	TPSODL/OT/2021-22/004 / 3.1 / 9	The bid must contain the name, residence and place of business of the person or persons making the bid and must be signed and sealed by the Bidder with his usual signature. The names of all persons signing should also be typed or printed below the signature.	Please provide the clarity regarding is there any digital signatures are required?	You can submit the bids with digital signature but should contain the details as mentioned in tender enquiry.
11	TPSODL/OT/2021-22/004 / 2.1 / 8	2.0 Evaluation Criteria 2.1 Price Variation Clause: The prices shall remain firm during the entire contract period.	The prices shall remain firm during the entire contract period subject to following conditions, a) No delay in contract execution because of TPSODL b) No change in scope of work/any other element of contract c) No default by TPSODL w.r.t contract	As per RFP
12	TPSODL/OT/2021-22/004 / 3.5.7 / 35	3.5.7 Hardware Minimum Support Period The Supplier shall guarantee the availability of spare parts and hardware maintenance support services for all System equipment for a minimum period of 10 years. Subsequent to this minimum support period, the Supplier shall provide to TPSODL a minimum of two year's advance notice of their intent to terminate such services.	We understand that this 10 years of period will start from date of LOI, please confirm	Date shall be start after completion of project.

Sr. No.	Detailed Reference to Tata Power Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
13	TPSODL/OT/2021-22/004 / GCC/5.0 / 12	5.0 PRICES/ RATES/ TAXES The Prices/Rates are inclusive of all taxes, levies, cess and duties, particularly Goods and Services Tax as applicable. All government levy / taxes shall be paid only when the invoice is submitted according to the relevant act. The prices/rates shall remain firm till actual completion of entire supply of goods/material/equipment as per contract is achieved and shall remain valid till the completion of the contract. The prices shall remain unchanged irrespective of TPSODL making changes in quantum in all or any of the schedules of items of contract.	1) In case project gets delayed due to reasons not attributable to the Associate, prices shall be re-negotiated and mutually agreed upon 2) The prices shall remain unchanged irrespective of TPSODL making changes in quantum in all or any of the schedules of items of contract. - Variation of +/-10% of individual items limited to +/-5% of contract value shall be acceptable. Any variation beyond this shall call for re-negotiation & mutual agreement on the item prices.	The price shall remain firm.
14	TPSODL/OT/2021-22/004 / GCC/6.5 / 15	6.1 Quantity Variation Payment will be made on the basis of actual quantity of supplies/actual measurement of works accepted by TPSODL and not on the basis of contract quantity.	The items which are supplied but not installed due to any reasons from TPSODL side, shall be paid in full.	Please supply the materials as per tender enquiry and payment shall be made only the materials supplied as per tender enquiry.
15	TPSODL/OT/2021-22/004 / GCC/3.6.2 / 36	3.6.2 Right to Change Software TPSODL must have the right to alter, modify, edit, and add to all software provided with the System. This right shall begin with the delivery of the Development system and the Supplier's baseline software. This requirement is necessary to facilitate development of TPSODL -supplied software and the interfaces to the other TPSODL computer systems. TPSODL agrees to discuss any changes to be made to software no less than 48 hours in advance of the implementation of the change.	TPSODL can make changes to software after the handover to TPSODL, however changes can be done at development server	As per RFP
16	TPSODL/OT/2021-22/004 / GCC/26.1 / 33	26.0 ATTRIBUTES OF GCC 26.1 Cancellation The Company reserves the right to cancel, add, delete at its sole discretion, all or any terms of this GCC or any contract, order or terms agreed between the parties in pursuance without assigning any reasons and without any compensation to the Associates.	We request you to delete this clause	As per RFP
17	TPSODL/OT/2021-22/004 / GCC/22 / 28	22.0 FORCE MAJEURE Force Majeure applies if the performance by either Party ("the Affected Party") of its obligations under Contract is materially and adversely affected. Act of war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy, embargo, blockade, revolution, riot, bombs, religious strife or civil commotion, etc. Politically motivated sabotage, or terrorism, etc. Action or Act of Government or Governmental agency for which remedy is beyond the control of the affected parties. Any act of God. Note: Causes like power breakdown/ shortages/fire/strikes, accidents etc. do not fall under Force Majeure.	Following events should be included as force majeure, any occurrence or event that is beyond the reasonable control of a Party hereto, fire, explosion & implosion, revolt, terrorism, earthquake, typhoon, other natural calamity strikes, floods, epidemics, quarantine restrictions	As per RFP
18	TPSODL/OT/2021-22/004 / GCC/3.7 / 6	3.7 Contract Price /Value The total all inclusive price/value mentioned in the PO/RC is the Contract Price/Value and is based on the quantity, unit rates and prices quoted and awarded and shall be subject to adjustment based on actual quantities supplied and accepted and certified by the authorized representative of the company unless otherwise specified in schedule of quantities or in contract documents.	"For all line items where payment is linked to Installation of SCADA/ADMS system, in case of delay due to TPSODL, then TPSODL will make payment within 15 days with respect to actual payment schedule."	As per RFP
19	TPSODL/OT/2021-22/004 / GCC/4.0 / 8	In the event, TPSODL requests a change, the Contract price and time shall be adjusted upwards or downwards, as the case may be and shall be mutually agreed to. The associate shall not be entitled to any extension of time unless such changes adversely affect the time schedule. The Associate shall not proceed with the changes as requested till adjustment of contract price and time schedule where so applicable in terms of or otherwise directed by the TPSODL	1) Change proposal to be approved by TPSODL within 7 days of submission of request by Associate 2) Associate also can request for change for approval by TPSODL 3) The contract price downward adjustment is not envisaged in this projects. TPSODL to confirm.	As per RFP
20		We request you to please include below mentioned clauses		

Sr. No.	Detailed Reference to Tata Power Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
		Extension of Time	1) Associate shall be entitled for extension of time for completion without imposition of liquidated damages under following conditions, i) Change in the Scope ii) Any occurrence of Force Majeure ii) Any suspension order given by the TPSODL iii) Any changes in laws and regulations iv) Any default or breach of the Contract by the TPSODL v) Any delay on the part of a Subcontractor, provided such delay is due to a cause for which the Associate himself would have been entitled to an extension of time vi) Delays attributable to the TPSODL vii) Any other delay beyond the reasonable control of the Associate 2) Associate shall be compensated for all the additional cost on account of such delays.	As per RFP
		Change in Law	Unless otherwise specified in the Contract, if after the Contract, any law, regulation, ordinance, order or by law having the force of law is enacted, promulgated, abrogated, or changed in India (which shall be deemed to include any change in interpretation or application by the competent authorities) that subsequently affects the Delivery Date and/or the Contract Price, then such Delivery Date and/or Contract Price shall be correspondingly increased or decreased, to the extent that the Associate has thereby been affected in the performance of any of its obligations under the Contract.	As per RFP
		Suspension by Associate	In case of TPSODL default, e.g.(Payment default, non availability of fronts, delay by TPSODL etc), Associate shall be entitled to suspend the completion of the Contract (and postpone accordingly the delivery schedule). In case of such event, Associate must not be considered in default and consequently must not be liable for any contractual sanction (such as penalty, liquidated damages, enforcement of performance bonds, termination for cause…).	As per RFP
		Labour Code	In case there is any increase in labour costs due to implementation of Labour Codes, the additional cost will be borne/reimbursed by the TPSODL to the Associate.	As per RFP
		Delay by TPSODL	Any delay by the TPSODL or its authorised agents for the reason not attributable to Associate shall lead to following, 1) Compensation on account of additional engagement of Associate manpower, tools, tackles and machineries 2) Compensation on account of additional expenses incurred by the Associate to run the site 3) Compensation on account of additional cost incurred by Associate for extension of insurance, bank guarantees etc. 4) Compensation on account of additional delay in receiving payments by the Associate. 5) Compensation on account of variation in commodity and labour prices. 6) Issuance of contractual delivery extension without imposition of LD within 15 days from the request by Associate	As per RFP
		Trade compliance - Export Control	TPSODL to comply with related applicable US, E.U. and other national and international export control laws and/or regulations and agrees to sign the End User Certificate in this regard. Proposed wordings: "The deliverables provided by Associate under this Contract contain or may contain components and/or technologies from the United States of America ("US"), the European Union ("EU") and/or other nations. Associate acknowledges and agrees that the supply, assignment and/or usage of the products, software, services, information, other deliverables and/or the embedded technologies (hereinafter referred to as "Deliverables") under this Contract shall fully comply with related applicable US, EU and other national and international export control laws and/or regulations. Unless applicable export license/s has been obtained from the relevant TPSODL and the Associate has approved, the Deliverables shall not (i) be exported and/or re-exported to any destination and party (may include but not limited to an individual, group and/or legal entity) restricted by the applicable export control laws and/or regulations; or (ii) be used for those purposes and fields restricted by the applicable export control laws and/or regulations. Associate also agrees that the Deliverables will not be used either directly or indirectly in any rocket systems or unmanned air vehicles; nor be used in any nuclear weapons delivery systems; and will not be used in any design, development, production or use for any weapons which may include but not limited to chemical, biological or nuclear weapons. If any necessary or advisable licenses,	As per RFP

Sr. No.	Detailed Reference to Tata Power Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
		COVID – 19 DISCLAIMER	TPSODL acknowledges that the GOODS supplied or Services performed or any part thereof may be produced in, sourced from, require personnel from or may otherwise be installed or performed in areas that may at any time be affected by the prevailing COVID-19 pandemic and that the situation may trigger stoppage, hindrance or delays in Associate's (or its SUBContractor'S) capacity to perform, produce, deliver, install or service the WORKS, irrespective of whether such stoppage, hindrance or delays are due to measures imposed by authorities or deliberately implemented by the Associate(or its SUBContractor's) as preventive or curative measures to avoid harmful contamination exposure of Associate's (or its SUBContractor's) employees. TPSODL, therefore recognizes that such circumstances shall be considered as a cause for excusable delay not exposing the Associate to contractual sanctions including without limitation delay penalties, liquidated or other damages or termination for default."	As per RFP

03. Tentative SCADA /ADMS Revised BoM

S. No.	Equipment		Berhampur (MCC)	Jeypore (BCC)	total
A	Server/ workstation Hardware with panel	Unit			
1234	**SCADA/ADMS server**	**No.**	**14**	**14**	**28**
	FEP server with interface switches	No.	12	12	**24**
	ISR server	**No.**	**2**	**2**	**4**
	NMS/Security server	**No.**	**2**	**2**	**4**
	DTS server	No.	5	5	10
	Developmental server	No.	5	5	10
	ICCP Server	**No.**	**2**	**2**	**4**
	Interface Server GIS	**No.**	**2**	**2**	**4**
	Web/Directory server	**No.**	**2**	**2**	**4**
	Workstation with dual TFT Monitors additional required for Berhampur, Aska, Bhnjanagar and Rayagada	No.	10	10	**40**
	Developmental console with dual TFT	No.	5	5	**10**
	DTS/Workstation Console with dual TFTs	No.	5	5	**10**
	DLP based Video Projection system with 2x3 Module configuration with each module at least 67" diagonal with common projector at MCC	No.	1	0	**1**
	80 Inch TV for Aska, Bhnjanagar, Rayagada and Berhampur circles	No.	1	1	**5**
	Storage & Backup Devices				
	External Mass storage device (for year online backup)	**No.**	**2**	**2**	**4**
	Exteranl DAT drive	**No.**	**2**	**2**	**4**
	Switches				
	Layer III switch (SCADA/DMS LAN)-48 ports	No.	8	8	**16**
	Layer III switch (Development system LAN)-24ports additional for Aska, Bhnjanagar and Rayagada	No.	4	4	**11**
	Security system (DMZ)				
	Firewall & network IDS/IPS	Nos	4	4	**8**
	Layer III switch	No.	4	4	**8**
	Other Active Devices				
	GPS Time synchronization system	Set	2	2	**4**
	Time, day & date digital displays	Set	1	1	**2**
	Printers				

	B/W Laser printer additional required for Aska, Bhnjanagar and Rayagada	Set	1	1	**5**
	Color Laser printer additional required for Aska, Bhnjanagar and Rayagada	Set	1	1	**5**
	Cabling System				
	Cable, Jacks etc. additional required for Aska, Bhnjanagar and Rayagada	Lot	1	1	**5**
B	**Software for Control Centre**				
	SCADA/DMS software	**Lot**	**7**	**7**	**14**
	ISR Software	**Lot**	**1**	**1**	**2**
	DMS software	**Lot**	**6**	**6**	**12**
	OMS software	**Lot**	**6**	**6**	**12**
	DTS software	Lot	5	5	**10**
	Developmental software	Lot	5	5	**10**
	Network Management Software/Cyber Security	**Lot**	**1**	**1**	**2**
	WEB server	**Lot**	**1**	**1**	**2**
	GIS Adaptor/Engine for importing data from GIS system	**Lot**	**1**	**1**	**2**

Note: - The above BoM are minimum requirement envisaged by Customer. Bidder can provide better configuration to meet the specification without Virtualization of hardware resources.

Specification: - 80inch TV

S.No.	Description of the Features	Specification
1	Display Size	80”
2	Light source	LED Backlight
3	Resolution	3840 x 2160 Pixels
4	Brightness (typ)	1800 cd/m2
5	Contrast Ratio(typ)	8000:1 Ratio
6	Response Time (typ)	8ms
7	View angle	160°(H) / 160°(V)
8	Life Time	100,000 Hours
9	View area	1860 (H) x 1046 (V) mm
10	Colors	200 Trillion
11	Interfaces	HDMI IN x 2, Display Port IN x 2, HDMI OUT x 1, VGA IN x 1, PC AUDIO-IN x 1, YPBPR IN(BNC) x 1, LAN IN x 1, AV IN x 1, AV OUT x 1
12	Control	RS232-IN x 1, RS232-OUT x 1
13	Speaker	10W x 2
14	Power	Voltage 100 V ~ 240 V, 50-60 Hz
15		Maximum <500 W
16		Standby ≤0.5 W
17	Environment	Operating Temperature 0°C ~ 45°C

18		Operating Humidity 10% ~ 90% RH Non-Condensing
19	Dimension & Weight	Product Size (W x D x H) 1947 x 60.5 x 1139 mm
20		Net Weight 50 Kg

Network Management System & Cyber Security Specification: -

12.1 **Network Management System & Security Information and Event Management (SIEM)**

12.1.1 Reliable, Secured and highly available communication infrastructure is the backbone for any real-time system used for remote monitoring and control, and connects geographically spread Sub-Stations with the Central Systems.

12.1.2 The network management software shall be based on the Simple Network Management Protocol (SNMP-Internet RFC 1157) over TCP/IP (CMOT), with additional proxy software extensions as needed to manage SCADA resources.

12.1.3 The NMS software shall provide the following network management capabilities:

a. Configuration management

b. Fault management

c. Performance monitoring

12.1.4 The network management software shall:

a. Maintain performance, resource usage, and error statistics for all of the above interfaces (i.e. servers, workstation consoles, devices, Routers, Layer-3 switches, telephone circuit interface equipment, and all SCADA gateways, routers etc.) and present this information via displays, periodic reports, and on-demand reports. The above information shall be collected and stored at user configurable periodicities i.e. up to 60 minutes. The Network Management System (NMS) shall be capable of storing the above data for a period of two years at periodicity of 5 minutes.

b. Maintain a graphical display of network connectivity to the remote end routers.

c. Maintain a graphical display for connectivity and status of servers and peripheral devices for local area network.

d. Issue alarms when error conditions or resource usage problems occur.

e. Provide facilities to add and delete addresses and links, control data blocks, and set data transmission and reception parameters.

f. Provide facilities for path and routing control and queue space control.

12.1.5 The network management platform proposed shall be capable of managing an infrastructure that consists of multi Bidder network elements. The Network management system shall facilitate following activities as per ISO network management model:

a. Fault Management to recognize, isolate, log and identify fault on network and connected machines, nodes, devices.

b. Performance Management to monitor system and network performance as specified

c. Configuration Management to collect information about computers in the system such as processors, memory, peripherals and processes running on computers and configuration aspects of network devices such as configuration file management.

d. Security Management to protect systems and network from unauthorized access, manage user access, authorizing rights and privileges
The network management software shall be based on the secured version of Simple Network Management Protocol (SNMP) for fault management and performance monitoring platform for long term performance management and trending. The NMS system shall have a simple browser-based user interface to provide all the pertinent information about the system. The user interface software shall be installed on all the Operator as well as programmer workstations. The NMS shall not impact the availability and performance of SCADA system and shall load not more than 3% any host CPU, 1% Network bandwidth and shall have secure communication. The Network management system shall monitor the performance, resource usages and error statistics of all the servers, workstations, routers and LAN devices, SDH multiplexers, etc. including for networks extension

12.1.6 Fault **Management**
The following functions shall be included:
a. Network discovery

b. Topology mapping of network elements

c. Event handler

d. Performance data collector and graphic

e. Management data browser

Each monitored device shall be represented by a graphical element on the management platform's console. Different colours on the graphical elements shall represent the current operational status of network/device. A graphical display for connectivity and status of servers and peripheral devices for local area network shall be provided.
The monitored devices shall be configured to send notifications (SNMP traps) to the NMS. The graphical element representing the device shall change to a different color depending on the severity of the notification received. The notification shall also be placed in a log file. The current version of MIB file of each of the devices shall be loaded on the NMS.
NMS system shall also be capable of handling RMON (Real-time monitoring) alarm and events from the critical network devices. RMON shall be generated in case of environmental factors (power supply, temp etc.) or resource utilization factor (CPU utilization, Bandwidth utilization etc.). Issue alarms when error conditions or resource usage problems occur.

12.1.7 **Performance Management**

The performance management part of NMS shall maintain performance, resource usage, & error statistics and present this information via displays, periodic reports, and on-demand reports. Including the following:

Utilization (CPU utilization as applicable) for
i. Servers, Workstations, Storage Devices

ii. LAN, Router, Switches

iii. Data Links
b. Bandwidth utilization for Routers/Switches Various interface statistics such as input queue drops, output queue drops, and ignored packets shall be connected from network devices to measure the performance level.

c. Memory utilization, Auxiliary memory I/O utilization, of
i. Servers and Other Machines

ii. Mass Storage Devices

Apart from real-time monitoring, the above information shall be collected and stored at user configurable periodicities i.e. 5 minutes to 60 minutes. The Network Management System (NMS) shall be capable of storing the above data for a period of two years at a periodicity of 5 minutes. The period over which the statistics are gathered shall be adjustable by the user, and the accumulated statistics shall be reset at the start of each period. The statistics shall be available for printout and display after each period and on demand during the period.

12.1.8 The Network Management System & Security Information and Event Management (SIEM) shall have the following major components:

12.1.8.1 Supply and implementation of Hardware along with OS for Network Management System (NMS) with 10 years warranty for Operational Technology Devices
12.1.8.2 Supply and implementation of Software for Network Management System (NMS) with 10 years warranty for Operational Technology Devices

12.1.8.3 Implementation of NMS Software for Operational Technology

12.1.8.4 Supply and implementation of Hardware along with OS for Security Information and Event Management (SIEM) with 10 years warranty for Operational Technology Devices

12.1.8.5 Supply and implementation of Software for Security Information and Event Management (SIEM) with 10 years warranty for Operational Technology Devices
Following are the major specification clauses / requirements which the Bidder has to consider in the offer and also provide compliance through confirmation on each of the below mentioned clauses

12.2. **NMS Monitoring Platform Requirements**

12.2.1.1 The proposed solution must support a multi - tier deployment architecture with distributed management servers for scalability purposes.

12.2.1.2 The proposed solution should be an integrated, modular and scalable solution from single OEM (i.e. all NMS components from single OEM)

12.2.1.3 The proposed monitoring solution should be configurable with Active Directory for authentication.

12.2.1.4 The proposed fault monitoring solution should provide capability to receive alerts/ alarms from all SNMP and non-SNMP based devices.

12.2.1.5 The proposed solution should be capable to provide hybrid monitoring architecture through support of both agent-based monitoring and agentless monitoring approach.

12.2.1.6 The proposed fault monitoring solution should provide capability to receive alerts/ alarms.

12.2.1.7 The proposed monitoring solution should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks e.g. initiating a script.

12.2.1.8 The proposed Solution should support distributed/ remote monitoring by installing additional management servers/ Hubs/ collectors at remote locations for scalability purposes.

12.2.1.9 The Central Monitoring system should be able to install on Windows or Linux Operating system platform

12.2.1.10 The Performance Reporting Portal should be web based with ability to define Accounts and Users for accessibility (RBAC).

12.2.1.11 The proposed monitoring solution should be capable to support distributed alarm handling capability across multiple monitoring domains.

12.2.1.12 The proposed monitoring solution should provide the ability to create custom dashboards for all monitored servers & devices.

12.2.1.13 The proposed monitoring solution should provide ability to monitor and generate alarms for set threshold for pre -defined monitored metrics

12.2.1.14 The proposed solution should provide web-based reporting interface with Top N reports (bidder has to specify the value of N) and functionality to define, customize and schedule analysis reports other than those available OOB. The following reporting dashboards must be available out of the box:
a. Top N Reports

b. Situation to Watch/Critical alarms

c. At a Glance/Bird eye view

d. Trend reports
The proposed solution must provide web-based interface for monitoring configuration

The proposed solution must allow distinct severity levels to be used for notification such as informational, warning, minor, major, and critical – to reflect levels of severity based on true criticality of alarm. The proposed solution must assign default severities to alerts based on observed Best Practices.
The proposed solution must provide dashboards that allow customizing to display historical data and real time info with charts, gauges, and other graphical elements.
12.2.1.15 The proposed solution must provide a portal that aggregates the overall performance information of all the management domains. The portal must be according to the modern web standards and support delivering rich content and flexible UI.

12.2.2 **Deployment Features**
12.2.2.1 The proposed fault management solution must support a role-based user access model that enables administrators to permit or restrict operator's access to different areas of information based on user security rights assigned.
The system needs to support concurrent multi- user access to the management system, enabling multiple read-write access to different areas of the management domain.
12.2.2.2 The system should have self -registration capabilities built into the product so that it can easily add support for new traps and generate alarms.

12.2.2.3 The proposed infrastructure fault management system must support all existing SNMP versions
12.2.3 **Network Discovery & Monitoring**

The Network Discovery Solution should provide visibility into network assets through highly accurate and real -time information about network infrastructure.
Network Discovery Solution should provide in - built ability to automatically discover & model layer 2/3 network devices, interfaces along with physical & logical connectivity between them with no / minimal user input and scripting.

Network Discovery module should provide:
a. Accurate automated network discovery and connectivity modelling

b. Visualization of discovered network

c. Active network inventory reporting

Network discovery solution should maintain an accurate representation of network
Network discovery solution should provide web - based reporting capabilities that allows users to quickly design, save & distribute reports, report templates and ad-hoc queries to view network asset information.
The Network Discovery Solution should be designed to provide network discovery and topology visualization for Layer 2 and Layer 3 networks, including IP, Ethernet services, and Multi-protocol label switching (MPLS), IPv4 and IPv6.
Network Discovery Solution should provide broad support to various layer2/3 network technologies such as MPLS IP VPNs, OSPF, BGP, EIGRP, VLAN, IP, HSRP, VRRP, CDP, Ethernet, Layer 2 Ethernet VPNs, IP over ATM.

12.2.4 The proposed system must support multiple types of discovery including the followings:
a. IP range discovery – including built-in support for IPv4/6 addresses

b. Import data - from pre-formatted files (IPs, ranges, strings or ports)

c. Trap-Based Discovery – whenever new devices are added with capability to exclude specific devices based on IP addresses / IP Address range
12.2.5 Proposed solution must be able to discover, model and create topology map of Virtual Port Channeling (vPC) or equivalent enabled devices and its vPC channels along with their individual physical port connections.

12.2.6 The Network Discovery Solution should include Web-based network topology visualization tool. The network visualization GUI should use the network topology to generate graphical maps of the network topology around particular devices and send these maps to Web clients on demand. It should also be possible to create network view based on user defined criteria to view/manage network assets better

12.2.7 The Network Discovery Solution should extend network inventory reports out-of-the-box and the capability to create custom reports through drag & drop or similar ability to create reports.

12.2.8 It shall automatically discover TCP/IP networks, display and build network topologies maps as soon as it is installed. Also, shall correlate and manage events and SNMP traps, monitor network health and gather performance data.

12.2.9 Proposed solution must be able to discover, model and create topology map of vPC (Virtual Port Channeling) or equivalent enabled devices and provide intelligent alarms, Root Cause Analysis (RCA) and Impact Analysis feature.

12.2.10 Proposed solution should provide VSS (Virtual Switching System) device discovery & modelling capabilities and provide advanced alarms and VSS related events correlations and management options.

12.2.11 Proposed solution must provide the virtual switch information / parameters like Chassis information (Chassis ID, Uptime, Role, Core Switch Priority, and Core Switch Preemp), VSL (Virtual Switch Link) Port Statistics, VSL Statistics, VSL connection information & Core Switch configuration.

The Network monitoring tool should support topology-based event correlation and root- cause analytics in turn, to help network operator's work more efficiently by focusing time and attention on root cause events.

12.2.13 Proposed NMS solution must be a native 64-bit or 32-bit application and thereby able to fully utilize the hardware resources (like CPU / RAM address space etc.) and create a highly scalable management platform that can provision for up to many thousands of network device management from a single optimized hardware for various applications. The NMS software must be a true 64-bit/32-bit application and thereby maximize the usage of available server resources and deliver good performance.

12.2.14 The Network monitoring tool should have the capability to create custom views of the network

12.2.15 The network monitoring module should support polling, like high polling frequency for critical devices, and normal frequency for non-critical devices.

12.2.16 In addition to various graphical views, the network monitoring module should also provide tabular views and folder views to quickly navigate the large networks.
The Network monitoring tool should provide network discovery, topology visualization, and root cause analysis for Layer 2 and Layer 3 networks, including IP, Ethernet services, and Multi-protocol label switching (MPLS), IPv4 and IPv6. The proposed solution should be able to support newer network virtualization technologies like SDN.
It shall do a proactive network and systems monitoring. With 24-hour-a-day, 7-day-a-week monitoring, so that administrators can identify and solve network resource problems before they occur, reducing down time.
12.2.17 The tool should capture each networks device's configuration, also the physical and logical connectivity between devices. The tool should model layer 2 and layer 3 network technologies including: Internet Protocol (IP), Ethernet, BGP, EIGRP, VRRP, HSRP, OSPF, VPN, VLAN, ATM and frame relay, MPLS, Layer 2 Ethernet VPNs (including virtual private LAN services and virtual private wire services), Protocol Independent Multicast, and Carrier Ethernet.

12.2.18 Network operators should be able to drill down on specific problems in the event list to locate the alarmed device in the network topology view or show a list of all outstanding alarms on a selected device in the network topology view.

12.2.19 The network monitoring module should support various event correlation.

12.2.20 **Network Fault and Performance Monitoring**
12.2.20.1 Fault monitoring module should provide Self - Service Dashboard that will allow to integrate event data into business and service views to create dashboards tailored to operations and management needs

12.2.20.2 Fault monitoring module should provide multiple visualization mechanism to view events such as folder view, tabular view. The visualization mechanism should also support ability to group events along with event summary.

12.2.20.3 Fault monitoring module shall receive all the alarms received from the various event sources, unifies them into a common alarm format, correlates them and provide a common graphical user interface for alarm analysis and acknowledgement.

12.2.20.4 Fault monitoring module shall be able to process all fault and event related information in real time. It shall be capable of processing in excess of 150 events per second during an event storm allowing visibility of all alarms.

12.2.20.5 Fault monitoring module shall consolidate, and de-duplicate repeated alarms collected from throughout the network and provide a clear, coherent and noise -free list of fault messages.

12.2.20.6 Fault monitoring module should be able to collect events from SNMP and non -SNMP management data sources, RESTAPI, databases, network devices, log files and other utilities. It should allow definition of custom rules for parsing / text manipulation, etc.

12.2.20.7 Fault monitoring module shall be able to filter off repeated alarms of the same device. The start-time, end-time of the alarm shall be indicated.

12.2.20.8 The system shall provide facilities that enable to determine the root cause underlying sets of alarms that exhibit certain patterns.

12.2.20.9 Fault monitoring module should have the capability to detect event rate anomaly – it should detect when it is receiving an unusually low or unusually high rate of events. The event rate should be compared to normal/ baseline and should generate a new event to describe the condition.

12.2.20.10 Fault monitoring module should have the capability to detect when it is subjected to an event storm based on user configured thresholds.

12.2.20.11 Fault monitoring module should have out-of-box capability to perform predictive analysis and generate events that represent predictions for systems that are in danger of an impending threshold violation, and which require attention.

12.2.20.12 Fault monitoring module shall be able to collect alarm events from all the managed Network Element via their respective element management systems or directly, if element management systems are not available for that equipment type.

12.2.20.13 All alarm messages shall be automatically recorded to a database in a form that enables easy and efficient future retrieval, query and analysis.

12.2.20.14 Fault monitoring module shall be able to present alarm history of selected devices for a specific period upon request.

12.2.20.15 All alarm/event messages shall be automatically time and date-stamped by the fault monitoring module as well as related information on (e.g. Alarm receive-time start-time, clear-time, acknowledge-time etc.) shall be logged.

12.2.20.16 Fault monitoring module should help to prioritize responses to alerts, manage escalation procedures using automated response policies.

12.2.20.17 Fault monitoring module should enable operators to define policies for handling incoming events through a graphical user interface

12.2.20.18 Fault monitoring module should be able to mark device / infrastructure under maintenance mode. It should have a GUI to define maintenance schedule.

12.2.20.19 Fault monitoring module shall provide a complete view of the health of the entire distributed environment from a centralized NMS console. It shall be able to provide decentralized management through multiple consoles with centralized escalation, reporting and control if required.

12.2.20.20 Fault monitoring module shall capture all the events that are generated across the multi Bidder network infrastructure, correlate them and automate suitable actions as defined.

12.2.20.21 Fault monitoring module shall trigger automated actions based on incoming events / traps through predefined message -actions definable in event management. It should integrate with proposed trouble ticketing system for auto ticket logging (to be provided by bidder).

12.2.20.22 The Solution must be capable of monitoring the availability, health, and performance of core networking devices including but not limited to CPU, memory, temperature, interface bandwidth utilization.

12.2.20.23 The solution should be capable of monitoring network delay/latency and delay variation

12.2.20.24 The solution should be capable of monitoring packet loss, Packet QOS, Packet Errors on one or more ports

12.2.20.25 The system should provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.

12.2.20.26 As fault monitoring is one of the most critical components, it should have inbuilt failover/redundancy mechanism right from the processing engine down to collection layer.

12.2.20.27 Fault monitoring module shall have easy -to-use graphical rules builder to help build and adapt business rules and automations quickly and easily. Rules shall be created using a GUI, which shall also provide a convenient environment for testing rules before they are put into production.

12.2.20.28 The tool should allow the operator to alter the monitoring policies that can be fine - tuned for a group of devices (each policy identifies the attributes of the device to poll to better understand the health of a device). It should also provide option to define a set of polling policies that adapt to changing network conditions.

12.2.20.29 Consolidated operations management system shall provide extensive library of integration adapters across various operations management systems, third party data & event sources. The integration adapters library should provide wide coverage:
a. Third party monitoring, event management, configuration management, business service management, databases, help desk/problem & incident management systems

b. Databases (like Oracle, DB2, Sybase, Informix, MySQL, SQL, ODBC etc.)

c. Event/Message Bus (like JMS, TIBCO, Vitria)

d. Standard Interfaces (XML, SNMP, LDAP, CORBA)

e. Custom applications (via command line, TCP/IP Sockets, flat-files, instant messaging, email)

12.3 **Fault/Alarm Management**

12.3.1 System should provide events & log analytics capability to analyze alarms via Dashboards, Custom Widgets etc.

12.3.2 The event / log analytics should leverage real - time alarm and alert analytics, combined with broader historic data analytics. It should provide event search and historical analysis in a single solution.

12.4 Advanced search and text analytics technology to search large amounts of: Alarms, Tickets, syslog, Logs data for quick troubleshooting.

12.4.1 It should provide data analytics, correlation capabilities based on ticket, alarms etc.

12.4.2 Search logs using configured and discovered patterns such as traces, class and event IDs, and error codes to quickly identify and repair issues.

12.4.3 Quickly visualize application error type distribution across thousands of log records.

12.4.4 It should provide the ability of keyword searches and should provide dynamic drilldown functions that allows to go deeper into the event data for detailed information.

12.4.5 The solution should provide Analytics capability to identify exclusive patterns within the monitored environment. It should use statistical analysis of historical event data to determine the seasonality of events, such as when, and how frequently events occur. The results should be presented in report and graphical format.

12.4.6 Analytics should be able to show time distributions of events and investigate pe ask so that user can trace the root cause of reoccurring seasonal events

12.4.7 Analytics should be able to better align thresholds to seasonal peaks which further reduces events.

12.4.8 Analytics should be able to detect events that are reoccurring regularly e.g. at a particular “hour of day”, “day of week” and “day of month” etc.

12.4.9 Solution should be able to generate alerts / alarms on pre-configured conditions.

12.4.10 Solution should integrate with LDAP / AD to provide Role Based Access Control so as to limit the exposure of logs based on user/ Operator roles.

12.4.11 System should be able to determine related events from the event archive and determine which alarms have statistical tendency to occur together and output the results on a scheduled basis as event groups.

12.4.12 The system should provide a related events dashboard which outputs the result of the analytics on a regular basis.

12.4.13 The dashboard should provide relative time differences between occurrences of related events so as to provide the operator a better understanding of the sequence of events leading to a service outage.

12.4.14 The solution should provide the ability to define rules that act on the event data and show a single parent event from the event group, with all other events in the group as children which in turn should reduce the number of events that are presented to operators.

12.4.15 System should provide Scope Based Event Grouping capability that allows to group alarms based on a defined scope.

12.4.16 The Scope should be defined as a Local or an Area scope. Local Scope could be based on one Device. Area scope could be based on the Links connecting two or more Devices.

12.4.17 The Scope should be defined in conjunction with a Time Window for grouping of alarms

12.4.18 The scoped Grouping visualization should be able to show the grouped alarms in parent child form.

12.5 **Network Configuration Management**

12.5.1 The proposed solution must have an in -built capability to carry out configuration management without the use of any external software to reduce integration efforts and increase ease of deployment.

12.5.2 The system should support secure device configuration capture and upload and thereby detect inconsistent “running”, “startup” or “reference” configurations and alert the administrators.

12.5.3 The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements: * Capture running configuration * Capture startup configuration

12.5.4 The proposed fault management solution must be able to perform real -time or scheduled capture of device configurations

12.5.5 The proposed fault management solution must be able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.

12.5.6 The proposed solution must support an approval workflow for network configuration management.

12.5.7 The Network Change & configuration management tool should provide the ability of data-driven templates that can be utilized to automate tasks that helps improve network integrity by enforcing configuration policies for regulatory mandates, security directives and engineering standards

12.5.8 Proposed solution should support multi Bidder network device configuration.

12.5.9 The Network configuration management tool should provide role -based access control that helps ensure that only approved users can access specific devices and perform upgrades.

12.5.10 The Network Change & configuration management tool should provide terminal that enable Telnet or SSH terminal access to devices. The tool should provide capability of session logging of all keystrokes and device responses and automatic backup of device activity after the session is terminated.

12.5.11 Solution should record / store the following data. Changes made to a device
a. Device change causes breach of policy

b. Event collected for changes and breaches

c. Root cause of faults identified

d. Remediation action taken

e. Root cause of breach fixed

f. Re-evaluation of change breach

g. What was changed on the device

h. Why was the change made

i. When was the change made

12.5.12 Auditing: Recording every access to a device including not only scripted and automated access, but a full keystroke log. Who made what change, the reason for the change and associated ticket number must be captured. Out-of-band changes must be detected.
The network change & configuration management key features should include the following:
a. Enables accurate and rapid configuration changes

b. Full Device Configuration Backup with Versioning

c. Full Configuration Search & Enable configuration comparisons across versions & devices too provide any Version to Version Difference

d. Offer direct command-line access to the device that is logged and auditable. Also permission setup should be possible, for example who can execute this function and which part of the network they can access.

e. Enforce change control process based on role and user access

f. Provide out-of-the-box and customizable reports

g. Provide back-up and restore of device configurations.

12.5.13 Should have compliance reporting that shows whether configuration comply with specific templates of configurations e.g. do they have the right ACL's, have they been configured with the correct service configurations.

12.6 **Network Traffic Analysis**
12.6.1 Proposed Network Traffic Monitoring should be a flow-based network traffic performance monitoring system.

12.6.2 It should provide a comprehensive and scalable visibility on network traffic with visualization and reporting of network performance data for complex, multi Bidder, multi - technology networks with increased visibility into total network performance.

12.6.3 It should help to perform analysis and visualization of network traffic for preventing network hogs and abuse.

12.6.4 Proposed solution should enable to effectively identify users, applications, interfaces, and, protocols that are traversing the network, which is consuming the most bandwidth in near real - time, through analysis and extensive visualization of data

12.6.5 It should help discover and analyze network traffic behavior patterns (on real time basis) such as:
a. Where bandwidth is used

b. Who is using it

c. How it is being used
12.6.6 Proposed solution should provide visibility and help to have improved control over end-to-end resource usage for hosts, servers, applications, protocols, interfaces.

12.6.7 Proposed solution should dynamically generate detailed network traffic reports from flow - information streams such as NetFlow, IPFIX, J -Flow, CFlow, SFlow and Net Stream.

12.6.8 Proposed solution should enable IT Network Operator to detect interface traffic threshold violations through identifying users, applications, interfaces, and protocols that are traversing the network, and identify the probable cause of the alert with the help of a single UI and consistent user experience. It should send alerts for threshold violations.

12.6.9 Proposed solution should provide built in DNS name resolution and should perform DNS forward and reverse resolutions to manage the Flow interfaces and resolve DNS names for reporting.

12.6.10 Proposed solution should be able to monitor minimum 25,000 flow records per second that are traversing the system.

12.6.11 It should provide traffic overview that delivers real-time, end-to-end, and scalable network traffic visualization with customizable features that meet our business requirements. It should also provide details of applications, hosts, and conversations consuming WAN bandwidth to isolate and resolve problems

12.6.12 Analytics component should perform flow session categorization and aggregation.

12.6.13 The proposed system must provide early warning of tunneling, rogue user behavior, host mis-configuration and other performance threats

12.6.14 The proposed system must comprise of baseline views and anomaly detection capabilities to identify abnormal traffic and analyze trends in applications, hosts, and conversations per QoS policy

12.6.15 The user interface should provide access to standard dashboards, which are pre - generated traffic reports for the fixed time periods such as Last Hour, Last Day, Last Week, Last Month etc.

12.6.16 The main grouping keys for the Network Traffic Overview dashboard should be definable as below specified grouping key:
a. Protocol

b. Source

c. Conversation

d. Application

e. Destination
12.6.17 It should provide the ability such that a new interface should automatically get added after receiving the NetFlow data from the exporter.

12.6.18 It should provide rich and adaptive features to display real time or near real -time dashboards, for quick analysis of data. The visualization features and capabilities should be as follows:

Near real-time flow monitoring
a. Should analyze the network traffic patterns

b. Should detect which applications are hogging maximum bandwidth.

c. Should provide simplified reports on detailed traffic data over a specified time period.

d. Ready to use traffic overview and traffic details dashboards

e. Should provide minimum ten network topology level dashboards for top 10 talkers

f. Should provide the drill down dashboards to device level or interface level for more details on flow

g. Bandwidth consumption by applications

h. Should be able to detect top applications usage of bandwidth.

i. Should be able to monitor their ports

j. Threshold values and alerting

k. Should provide traceable alerts that are sent instantly when an interface crosses the configured threshold value.

l. Should provide help to drill-down to the interface that exceeds its threshold value.

m. Historical Data

n. Should provide configurable flow data from a specific date or time to view activity and problems in the captured data. Flow data should be available from Following widgets at minimum should be integrated in Traffic Overview dashboard
12.6.19 Following widgets at minimum should be integrated in Traffic Overview dashboard:
a. Top Interfaces

b. Top Ingress Interfaces

c. Top Egress Interfaces

d. Top Applications

e. Top Protocols

f. Top Conversations

g. Top Sources

h. Top Destinations

i. It should provide the ability to view the traffic details of a particular entity both at Network and Interface levels.
12.7 **Server & Database Management**
The solution should have the following features:
a. Scalable and resilient monitoring across the infrastructure domain

b. Hybrid monitoring architecture through support of both agent-based monitoring an agentless monitoring approach

c. Single solution for visibility and intelligently managing applications & application infrastructure in classic, virtualized, cloud and hybrid environments

d. Monitoring all critical components at server, OS, application & database level – such as server resources, virtualization technologies, applications, web server and databases etc. Should be able to monitor various industry - wide popularly used Operating Systems & Virtual Environment, Databases & Web Servers.
12.7.1 Web dashboards should be available to identify fy, isolate, and diagnose availability, performance, and capacity issues. Web dashboard should be role-based.

12.7.2 User Interface for improved visibility into the application environment, for quicker problem isolation and root cause identification, and is viewable on smart devices.

12.7.3 It should provide capability to build unique monitoring solution agents for home grown or custom applications. It should facilitate creation of custom agent using a wizard along with the capability to integrate with web base portal so as to visualize and collect real time and historical data from custom agents.

12.7.4 It should provide Adaptive baselining capability which allows the system to learn the normal range of values for a given metric based on its history.

12.7.5 It should provide capability of fixed and Dynamic thresholds (Without restart) which allows thresholds to be set from learned behaviour based on the history of the specific resource or metric. These thresholds can vary based on the behaviour of the relevant metric and can change by hour, day or another appropriate time period.

12.7.6 It should provide predictive alerting capability when a dynamic threshold is crossed so as to alert administrator that something abnormal is occurring and should be reviewed. At this point an outage has not occurred or the relevant performance metric is outside its normal bounds and an outage or degradation could occur.

12.7.7 It should provide linear Trending capabilities to allow users to view directional trends of performance metrics. It should also provide capabilities to set policies to kick off predictive alerts when it looks like a trend will exceed a threshold within a given timeframe

12.7.8 It should monitor physical resources that have been abstracted and pooled by a virtualization hypervisor for sharing among virtual machines and clusters.

12.7.9 It should provide health dashboards for rapid assessment of infrastructure health & performance.

12.7.10 Systems Management should enable the selection of Key Operational Metrics that provide the best indication of operational performance and capacity.

12.7.11 The Monitoring tool should support monitoring of standard RDBMs like Oracle, MS-SQL, Sybase, Informix and DB2.

12.7.12 The Database monitoring should seamlessly integrate with the same (NMS) Dashboard/Portal and provide integration with the central event console.

12.7.13 It should provide monitors with pre -set thresholds and automatic corrective actions for DB2, Oracle, MS-SQL, Informix and Sybase databases.

12.7.14 The solution should be able to monitor servers using WMI and SSH.

12.7.15 It should enable users to manage multiple databases across different platforms from a central console with single product and a consistent architecture.

12.7.16 It should support a central repository for historical and real -time reporting that enables trend analysis data to better plan the resource utilization.

12.7.17 It should easily integrate into an end -to-end enterprise management solution.

12.7.18 All data captured by the monitors should be delivered through an intuitive user interface and made available through historical and real -time reports.

12.7.19 It should provide the ability to define custom situations, thresholds, and tasks that can be defined, by the DBA, based on the best practices.

12.7.20 It should facilitate administrators to view the database and system environment with a single Web-accessible interface and perform administrative tasks from any location.

12.7.21 The tool should provide the ability to easily collect and analyze specific information, including information on:
a. Buffer pools

b. Databases

c. Server key events

d. Tablespaces

e. Database Usage

f. Database State

g. Errors
The monitoring tool should provide pre -defined views and enable the admin to easily define new workspaces with metric collections based on their own best practices. These workspaces should be reflected in the enterprise portal.
The Solution should Provide query's Response Time for Monitoring Custom Queries
Database Space Monitoring for both file group and transaction log (Warning threshold, Critical threshold as well as file group/log full)
The solution must support Database Health and Settings - Check database status (offline, suspect), Check database options (auto grow, auto shrink, auto close etc.)
The solution should support auto-discovery of database instances.
The solution should support the creation and management of reusable test templates that contain a specific pre -defined set of database checkpoints/measurements.
12.8 **Application Performance Management**
12.8.1 The bidder should provide an integrated solution for monitoring across a broad set of heterogeneous application infrastructures. It should provide one tool for monitoring, viewing, analysing, forecasting and managing applications running on Physical as well as Virtual Environments across the enterprise consolidating critical application data in one easy-to-use Web Based Portal

12.8.2 It should help manage business applications by proactively monitoring essential system resources, detecting bottlenecks and potential problems and automatically responding to events.

12.8.3 It should be built on the highly scalable distributed architecture and provide efficient, centralized management of distributed and
Web-based systems.
12.8.4 The proposed solution should support and be installable on industry standard RDBMS like Oracle/ MS-SQL/ DB2/ Sybase/ Informix etc. and licenses of RDBMS should be part of the proposed solution.

12.8.5 The proposed system must be able to detect user impacting defects and anomalies and reports them in real -time:
a. Slow Response Time

b. Fast Response time

c. Low Throughput

d. Partial Response

e. Missing component within transaction
12.8.6 The proposed system must be able to pro - actively determine exactly which real users were impacted by transaction defects, their location and status

12.8.7 The proposed system must provide the ability to detect and alert when the application is not available

12.8.8 Solution shall be able to monitor customer transaction by end-user name, and thus able to understand exactly which customers were impacted, their location, type of browser used etc.

12.8.9 Solution must be able to extract data from Http request header and body to assist in identifying transactions or extract user, session and other parameters.

12.8.10 It should provide reporting capability so as to access critical information for better and more proactive business decisions

12.8.11 The proposed solution must determine if the root cause of performance issues is inside the monitored application, in connected back -end systems or at the network layer from a single console view.

12.8.12 The proposed solution must proactively monitor 100% of real user transactions; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.

12.8.13 The proposed solution must provide deeper end-to-end transaction visibility by monitoring at a transactional level and without deploying any software at end user desktop.

12.8.14 It should provide integrated performance and capacity management to monitor, alert and report on future capacity bottlenecks

12.8.15 It should provide end-to-end monitoring for:
a. Operating systems including AIX, Microsoft Windows, Linux, Solaris, HPUX, AS400, i5/OS etc.

b. Virtualization including all industry standard layers such as VMWARE, Hyper-V, PowerVM, RHEV, OVM etc.

c. Database servers including DB2, Oracle, MS- SQL, MYSQL, Sybase, Informix and unstructured databases etc.

d. Web resources including web servers (such as IIS, Apache, etc.) application servers, Java™ Platform and Enterprise Edition (Java EE) applications, J2EE platforms, WebSphere, WebLogic, SAP NetWeaver
12.8.16 It should have simplified installation and configuration. It should be possible to deploy and update the agents remotely.

12.8.17 The agent should provide a store and forward capability, it should be recoverable and can continue to function after the network is restored.

12.8.18 It should offer an easy, consistent way to monitor and manage key distributed resources through a centralized management interface. Monitoring parameters should be able to set and updated for an entire group and applied to distributed resources in a single action.

12.8.19 The tool should provide facility for benchmarking server performance and alerting on abnormal behaviour rather than relying on just fixed thresholds.

12.8.20 The proposed solution should detect performance hotspots in the applications.

12.8.21 The proposed solution must provide a single view that shows entire end-to-end real user transaction and breaks down times spent within the application components, SQL statements, backend systems and external 3rd party systems.

12.8.22 The proposed solution must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.

12.8.23 It should provide role -based, real-time views of monitoring data, allowing problems to be viewed in the context of the application and historical context which in turn enables quick drill-down to determine the source of a problem. It should provide side-by-side real time and historical views, expert advice and automated best practice s in response to incidents.

12.8.24 It should provide role -based, real-time views of monitoring data, allowing problems to be viewed in the context of the application and historical context which in turn enables quick drill-down to determine the source of a problem.

12.8.25 The tool should facilitate development of monitoring agents for home grown or custom applications. It should be able to create a custom agent using a Wizard or equivalent methodology

12.8.26 It should enable proactive management of transactions, identifying bottlenecks and other potential problems for standard applications.

12.8.27 It should support synchronous and asynchronous message tracking

12.8.28 It should support an agent based as well as agent-less Web response monitoring component that allow us to adopt an end user’s perspective when measuring transaction performance. The software should enable us to capture performance data from real Web-based transactions.

12.8.29 It should deliver unparalleled support across distributed infrastructure

12.8.30 It should proactively recognize and isolate transaction performance bottlenecks in complex composite applications along with intelligent alerts based on user defined thresholds

12.8.31 It should deliver response time monitoring of both real-user and synthetic transactions

12.8.32 It should provide the ability to measure the performance of HTTP and HTTPS requests including performance information for objects embedded in a Webpage. These measurements should include a number of dimensions, including total response time, client time, network time, server time, load time and resolve time.

12.8.33 It should provide application console to see status summary and trend analysis information across managed resources and to perform problem determination

12.8.34 It should collect data in real time at a configurable, constant interval.

12.8.35 It should provide accurate status directly from the monitoring agent situations.

12.8.36 It should provide the ability to fully customize the reports.

12.8.37 It should show the overall status of monitored Internet services by host, user profile, and service type.

12.8.38 It should be capable of monitoring all the following Internal services:
a. DHCP

b. ICMP

c. RADIUS

d. SNMP

e. Dial

f. IMAP4

g. RPING

h. SOAP

i. DNS

j. LDAP

k. RTSP

l. TCP Port

m. FTP

n. NNTP

o. SAA

p. TFTP

q. HTTP

r. NTP

s. SIP

t. WMS

u. HTTPS

v. POP3

SMTP

x. And other standard IT & OT services and protocols

12.9 **Report/Service Log**

12.9.1 It should provide the ability to view a list of related records and view the work and communication logs for all related records on one screen, on the global record.

12.9.2 Solution should be able to deliver the business Intelligence reports.

12.10 **Incident Logs/Reporting**

12.10.1 It should provide the ability to create an incident record to document a deviation from an expected standard of operation.

12.10.2 The proposed solution shall provide classification to differentiate the incident via multiple levels/tiers of categorization, priority levels, severity levels and impact levels.

12.10.3 The proposed solution shall provide the ability to associate each incident with multiple activity log entries via manual update or automated updates from other security or infrastructure management tools.

12.10.4 The proposed solution should provide various escalation policies for multiple escalation levels and notification to different personnel via e -mail

12.10.5 The proposed solution shall provide status of registered incidents to end-users over email and through web

12.10.6 It should provide the ability to view a list of related records and view the work and communication logs for all related records on one screen, on the global record.

12.10.7 It should provide the ability to identify a global incident which is the root cause of many other issues or that is something affecting many users.

12.11 **Change Management**

12.11.1 The proposed solution shall support version control for Configuration Items.

12.12 **Reporting / Dashboard**

12.12.1 The proposed solution shall provide commonly used standard out of the box Reports.

12.12.2 The Proposed solution should provide native capability to deliver Business reports

Reporting tool should provide the ability to send reports via email with interactive features like clickable charts, sorting, radio button, tabs, cascading lists, checkbox filtering etc. It should provide the output in PDF, Excel and CSV formats.

12.12.4 The proposed solution should provide a web - based reporting solution that provides role - based access to existing report content, creation of new reports.

12.12.5 Based on the style of report that is selected, it should provide the facility so that the summaries can be displayed at the header or the group level. The summaries should provide high level overviews including counts, averages, minimum values, maximum values etc.

12.12.6 Reporting tool should provide reports enabling historical views of availability, utilization, performance and other key metrics.

12.12.7 The solution should provide flexible report formats.

12.13 **Collaboration and Mobility**
12.13.1 The Proposed Solution should provide the ability to broadcast message to all users.
12.14 Bidder to consider Redundant Centralized NMS with Hardware, Networking Accessories such as Network Switch, Cables, LIU's, Patch cords, etc. and NMS Software license for 10000 Nodes. The NMS Hardware + Software + OS shall be housed in Pre-wired server Panel (size 42U), rack mounted server systems, KVM switch, Sliding Monitor, Keyboard and Mouse along with other accessories

12.15 Testing & Configuration of Network Management System with the facility to monitor the network, consolidate the device logs and provide system wide user authentication.

12.16 Configuration changes in installed existing Automation WAN Network across Purchaser Network for seamlessly accommodating the new supplied system.

12.17 Bidder to consider the Time synchronization of the Network equipment with Purchaser's substation GPS receiver on SNTP. If the same is not supported by the proposed system, the bidder shall consider the alternate solution for time synchronization of the communication network components

All bidders to note that

'As per RFP there are two physical locations, one is MCC and other is BCC. The servers are inclusive of Rack and KVM switches as per configuration requirement.

The above statement supersedes all earlier communication / clarification regarding Rack and KVM switches.'

--- END of Document ---