Corrigendum- 2

Consolidated replies to the pre bid querries

FORMAT B.1
Format for Technical Pre-Bid Queries
Tender No **Tender Enquiry No- TPSODL/OT/2021-22/004**
Package Name **SCADA and ADMS System**

Sr. No.	Detailed Reference to TPSODL 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	Volume 1, Section4, 4.6 Technical solution Evaluation/ Page No 42	Purchaser shall provide GIS data for Distribution network modelling to bidders one month prior to pre-demo preferably TPCODL to test compatibility	We request TPSODL to provide the GIS data as soon as the bid is submitted/bid submission closing date, so that any clarifications/additional data requirements can be handled depending on the network connectivity and attributes as seen in the ADMS system after the import and subsequently prepare the demo system. Kindly confirm.	purchaser's will provide GIS data or in absence of GIS data, bidder will use the sample GIS data for demonstration
2	Volume 2, 1.3 Scope of work/page No 46	Providing source code for customizations	Installation software and backups will be provided to TPSODL which can by used by their engineers to do a complete software installation/restoration by TPWODL. Further, the integration with external systems will be done on open interfaces like ODBC, OPC & API and will ba part of the configuration. Hene request TPSODL to delete this clause.	as per the RFP.
3	2. SCADA/ADMS Architecture/page No 49	NOTE:- SCADA/ADMS, ISR, COMMNUICATION, FEP, NMS, DMZ, WEB SERVERS SHALL BE DUAL REDUNDANT. SCADA /ADMS LAN SHALL BE DUAL STAR TOPOLOGY & DTS, DEVELOPMENT SYSTEM, BCC SHALL BE SINGLE SYSTEM.	While its mentioned that DTS, DEVELOPMENT SYSTEM, BCC SHALL BE SINGLE SYSTEM, the architecture diagram and the BoQ in pages 285 and 286 is not reflecting the same. Please clarify.	BCC shall be replica of the MCC
4	2. SCADA/ADMS Architecture/page No 50	System Architecture The operation philosophy will be as followed: Berhampur, Berhampur City i.e., MCC location and Sambalpur of TPWODL or Jeypore i.e., BCC with full function operation. The Rayagada, Bhanjnagar and ASKA will be de-centralized remote locations for area power system control center.	We understand that the MCC and BCC will have complete system with servers and workstations, while the 3 remote centers at Rayagada, Bhanjnagar and ASKA circles will be remote workstations connected to MCC/BCC. Further we understand that the MCC and BCC locations mentioned - Berhampur and Sambalpur are locations for TPSODL SCADA/ADMS and not TPWODL as mentioned. Please confirm.	As mentioned in document, BCC can be located in Sambalpur(TPWODL)
5	2.2.2 Database development tools/page No 56	The bidder would submit the report of CIM certification testing with other vendor's product along with the bid. The database tool should have the facility to export and import model files as per IEC 61970 part 552-4.	IEC 61970 is the CIM standard for transmisison network and not applicable for the ADMS. Further there are no conformance test cases and certifications with regards to the ADMS and also there is no clarity on testing with other vendor's product based on the project scope. Hence request TPSODL to delete this clause.	as per RFP

Sr. No.	Detailed Reference to TPSODL Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
6	2.6.4 Interfaces (External)/page no 70	SCADA/ADMS system and network must compliance all the controls of ISO27001:2013	ISO27001 is the standard for IT security management system and is applicable for the compliance within the organization for the assets/information owned by them. This does not cover the Industrial control system/OT systems and is not applicable for a project delivery. Hence request the same to be deleted.	Bidder has to assist customer to make complaint to ISO27001 standard for MCC & BCC activity
7	2.7.1.2 SCADA/ADMS from GIS Interface/page no 71	As part of this interface GIS adaptor would be required for GIS Land base data, network model using GIS engines/adaptors supporting Native Adapters , CIM/XML Model for Distribution / Power System, using Model Exchange & Data Exchange over IEC 61968 Enterprise SOA Based BUS.	Please provide the details of the GIS system - The GIS vendor and the GIS software version.	this is under Procurment process and shall be CIM/XML compatible.
8	Page No 73	Table 2-1: SCADA/ADMS Redundancy and Table 2-2: User Interface Equipment	These tables are not clear w.r.t the architecture diagram and the BoQ and also the non-redundant requirement mentioned as "Note" in Page 49 of 290 in the architecture diagram.	BCC shall be replica of the MCC in point of functionalities, servers & network.
9	Appendix – D SCADA/ ADMS Bill of Material/page no 285	The No. of servers mentioned are 10 each at MCC and BCC for the following types- SCADA/ADMS, FEP, ISR, NMS, Interface Server; 5 each at MCC and BCC for DTS and Development Server	With this BoQ the total servers required are 120 Nos. Please clarify the utilization and confirm the requirement of these many no. of servers servers. Also this is not corresponding to the architecture diagram in page 49 of 290	**Refer Revised BoM**
10	Appendix – D SCADA/ ADMS Bill of Material/page no 285	The No. of workstations/consoles are 5 each at MCC and BCC for Development and DTS consoles and 10 each at MCC and BCC for workstations and additional 15 workstations for Aska, Bhanjnagar, Rayagada and Jeypore	With this BoQ the total workstations/consoles required are 55 Nos. Please clarify the utilization and confirm the requirement of these many servers. Also this is not corresponding to the architecture diagram in page 49 of 290.	**Refer Appendix D**
11	Appendix – D SCADA/ ADMS Bill of Material/page no 285	Storage & Backup Devices - The external mass storage device and Exteranl DAT drive are mentioned as 5 each at MCC and BCC	With this BoQ the total online storage and external DAT drive are 10 Nos. each. Please clarify the utilization and confirm the requirement of these many servers. Also this is not corresponding to the architecture diagram in page 49 of 290.	**Refer Revised BoM**
12	Appendix – D SCADA/ ADMS Bill of Material/page no 285	Switches and Security system (DMZ)	1) Please clarify the quantities of the switches as they are not corresponding to the architecture diagram in page 49 of 290 and also the architecture diagram does not indicate LAN segmentation b/w SCADA and development system LAN. Also, if there is segmentation each LAN will require only 2 switches.	Conceptual architecture Proposed by Customer . Bidder has to provided actual architecture to meet the functonality, operation philoshphy and availbility of SCADA/ADMS system
13	Appendix – D SCADA/ ADMS Bill of Material/page no 286	Printers	B/W and Color Printers are mentioned as 1 set each at both MCC and BCC with additional required for Aska, Bhanjnagar, Rayagada and Jeypore. The total is mentioned as 5. Please confirm specific quantities of printers at each locations to be considered.	as per the RFP.

Sr. No.	Detailed Reference to TPSODL Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
14	Appendix – D SCADA/ ADMS Bill of Material/page no 286	Software for Control Centre	All software is mentioned in Lot as 5 each in MCC and BCC for each of the software - SCADA software, ISR software, DMS software, OMS software, DTS software, Development software, NMS, WEB /Network security software and GIS Adaptor/Engine. The requirement of 5 each in MCC and BCC is not clear. Please clarify and confirm the quantities.	**Refer Revised BoM**
15	TPSODL/OT/2021-22/004/1.3/46	Study of existing deployed Micro SCADA and migration along with interfaces planned by TPSODL	Kindly provide details about existing Micro SCADA system and what all data need to be migrated to new SCADA/DMS system	SCADA/ADMS implementer will migrate the data from Micro SCADA system to be placed at centre location. There will be approx. 100 nos out of 254 nos of PSS at Micro SCADA.
16	TPSODL/OT/2021-22/004/2/50	Communication link between MCC and BCC and between MCC,BCC and de-centralized remote location	Kindly provide communication link bandwidth available between MCC,BCC and de-centralized remote location. Minimum 100 mbps communication link is recommended over here. Also to facilate autosync between MCC & BCC, minimum 1 gbps communication bandwidth is recommended between MCC & BCC. Please confirm.	The successful bidder will provide requirement during engineering based on actual requirement TPSODL will arrange communication link however basic communication infrastructure mentioned in Table 2.3
17	TPSODL/OT/2021-22/004/2.2.3.4/59	The Contractor shall arrange the required software tool to acquire the initial data from the existing control centre at his own cost.	Please clarify in which format data from existing system will be provided.	Bidder need to analize the data and propose the applicable format. As of now LDMS and Local Monitring available
18	TPSODL/OT/2021-22/004/5/113 and 286	The bidders are encouraged to optimize the requirement of hardware for servers and processors where one or more applications can be combined or distributed in any combination with adequate redundancy without impacting the performance as described in section 3. However certain applications are to be hosted on independent hardware. Note:- The above BoM are minimum requirement envisaged by Customer. Bidder can provide better configuration to meet the specification without virtualization of hardware resources.	Above two clauses are contradictory to each other. However, we request you to confirm that the Bidders can optimize the BoQ as per their solution offering.	The hardware quantity are minimum however based on application requirement Bidder can optimise the resources to meet the performance and availability.
19	TPSODL/OT/2021-22/004/9/179	The Simulator shall include the functionality listed in Table 9-1 Documentation, Quality Assurance and Testing , Project Implementation	Please clarify what is expected from simulator in terms of Documentation, Quality Assurance and Testing , Project Implementation	Please refer respective section in the RFP.
20	TPSODL/OT/2021-22/004/2/48	Sizing	Kindly provide sizing in terms of no of RTUs, FRTUs, digital points. Analog points etc to be integrated with new SCADA/ADMS system.	Refer Appendix - C
21	TPSODL/OT/2021-22/004/2.7.1.2 /71	As part of this interface GIS adaptor would be required for GIS Land base data, network model using GIS engines/adaptors supporting Native Adapters , CIM/XML Model for Distribution / Power System, using Model Exchange & Data Exchange over IEC 61968 Enterprise SOA Based BUS.	Please provide details about GIS system wrt 1. Make & Model 2. All data format in which electrical and attribute data will be available from GIS system 3. Format in which landbase data will be available from system	Detail shall be provided during engineering phase
22	TPSODL/OT/2021-22/004/2.7.1.5/72	There will be an interface between the SCADA/ADMS and the work management system (WMS) to create work orders/switching orders for planning different types of planned shutdowns.	Please confirm if integration betrween SCADA/ADMS system and WMS system can be done over SOA based web services?	Integration between SCADA/ADMS system and WMS system can be done over SOA/ web services.
23	TPSODL/OT/2021-22/004/2.7.1.8/72	SCADA/ADMS should be equipped with in-built interface developed with 3rd party Data Historian (such as PI, E-DNA, Hadoop, SAP-HANA etc.) which will send data on real time basis to Historian.	Please provide make & model of historian system with which SCADA/ADMS system is expected to be integrated.	to be discussed during engineering phase

Sr. No.	Detailed Reference to TPSODL Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
24	TPSODL/OT/2021-22/004/1.2.2/25	Archival Storage for DMS & OMS	Separate Archival Storage for DMS & OMS is mentioned but there is no qty mentioned in BOQ. It is requested to add Storage with quantity in BOM	Refer Appendix - D, the External Mass storage device (for year online backup)
25	TPSODL/OT/2021-22/004/1.2.5/26	Backup Control System	There is a inconsistency in requirement of VPS between 1.2 Hardware Prices with BOM. Kindly confirm that 80inch TV need to be provided or VPS at BCC?	80inch TV need to be provided at BCC & LDC location.
26	TPSODL/OT/2021-22/004/2.7.1.8/72	Backup Control System Operations consoles 2 monitor (BCS) optional other location (80 inch TV)	There is a inconsistency in requirement of 80inch TV with BOQ. Kindly confirm that 80inch TV need to be provided at BCC.	80inch TV need to be provided at BCC & LDC location.
27	TPSODL/OT/2021-22/004/3.1.3/80	Fifty percent of the auxiliary memory capacity of each processor, console, or storage unit shall be unused (spare), and completely available for future use by TPSODL	To meet the requirement of fifty percent of the auxiliary memory capacity of each processor, we request to modify the requirement of Hard Disk on Server to 2TB on RAID 1.	as per the RFP.
28	TPSODL/OT/2021-22/004/5.5/118	The time and frequency facility shall include digital displays for: 1) UTC time and date in the format DD:HH:MM:SS (the hour display shall be in 00 to 23 hour format) 2) Time deviation in the format ±xx.xx seconds 3) Power system frequency in the format xx.xxx Hz 4) Frequency deviation in the format ±x.xxx Hz.	Frequency Deviation, Time Deviation as well as Power system frequency is mentioned where as in case of 5.11 page number 117 (Digital Display Clock). It is not mentioned in BOQ. Kindly amend the same. Kindly provide architecture for GPS connectivity with Digital Display Clock.	Refer Appendix - D
29	TPSODL/OT/2021-22/004/5.6.1.1/119	Monitors	There are two different Monitor specs provided kindly confirm which to refer. Minimum refrest rate 75Hz is applicable for Gaming Monitors and standard refresh rate for SCADA environment is 60Hz. Kindly confirm & change the same.	Pls refer section 5.11 Table-A of RFP
30	TPSODL/OT/2021-22/004/5.6.1.1/119	Workstation consoles for development system shall also be available with single TFT monitor Operator	The requirement for development workstation is with single TFT monitor , while in te BoQ Pg 266/424 have asked for Developmental console with dual TFT. Kindly confirm the TFT requirement for development workstation.	Pls Refer BoQ.
31	TPSODL/OT/2021-22/004/5.11/124	Hard Disk Drives : SATA 1 TB	Kindly confirm that Hard Disk Drive in RAID 1	as per the RFP.
32	TPSODL/OT/2021-22/004/5.11/124	1. Servers Additional port : Server should support 2 Number of 10G Fiber Ethernet Ports with SFP	We could not see the connectivity to the Control Center LAN on 10G Fiber. Hence, we request you to remove 10G ports from the Servers.	as per the RFP.
33	TPSODL/OT/2021-22/004/5.11/124	1. Servers	Since the Bidders are encouraged to optimize the overall solution, we can also optimize the Server Configuration provided in the tender. Kindly confirm.	as per the RFP.
34	TPSODL/OT/2021-22/004/7/128	Layer-3 switching & VLAN	The request in TABLE 5 there is 48 Port L3 Switch , while in the BOQ Sheet (Pg 266) asked for 48 / 24 Ports L2 Switch	48 Port L3 Switch will be in production however for devlopment / 24 Ports L2 Switch will be prefered.
35	TPSODL/OT/2021-22/004/8 and 9/128 and 131	9. SAN Switch	It is requested to add quantity of SAN Switch in BOQ.	This is included in SAN Storage
36	TPSODL/OT/2021-22/004/10/131	Interface ports: Suitable port for interfacing with servers/workstations.	Tape Library is suitable to inteface with Server and not to workstation. It is requested to remove the requirement from workstation.	Tape Library shall be used for servers
37	TPSODL/OT/2021-22/004/10/131	Tape Library	Kindly provide minimum native capacity required on Tape Library.	
38	TPSODL/OT/2021-22/004/10/131	Tape Library	Request for deletion of LTO-3-060, LTO-3, LTO-4-120, LTO-5-140 which is EOL. Now Tape libraries support LTO 6 LTO7 LTO 8.	Refer Tape libraries LTO 6 LTO7 LTO 8.
39	TPSODL/OT/2021-22/004/2/125	Graphic adapter cards(HDMI/DVI/Display Port)	It is recommended for all workstations to have minimum 4GB Nvidia Graphic card for better performance.	as per the RFP.
40	TPSODL/OT/2021-22/004/5.6.1.1/119	Diagonal Viewable size 24”	Typically 24inch monitor available from standard OEM come with diagonal viewable size is 23.5inch, kindly confirm the same is acceptable.	as per the RFP.

Sr. No.	Detailed Reference to TPSODL Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
41	TPSODL/OT/2021-22/004/5.6.1.1/119	Anti-glare & anti-static	The required feature is applicable to CRT monitors and not to TFT Monitor, Kindly remove the same.	as per the RFP.
42	TPSODL/OT/2021-22/004/2/125	Dual AC Power Supply (in Watts)	Kindly confirm dual power supply is not applicable for Desktop mounting workstation as it is not manufactured by OEM.	as per the RFP.
43	TPSODL/OT/2021-22/004/3/126	Overall brightness of each module : Minimum 2400 ANSI Lumens	Here we understand brightness onscreen mentioned can be achieved with lower Lumens module and it is provided OEM specific. Since it is mentioned DLP Technolog : LED and 2400Lumens is available only in laser so kindly remove the same.	as per the RFP.
44	TPSODL/OT/2021-22/004/4/126	VPS Controller Feature	It is recommended for VPS Controller to have minimum 4GB Nvidia Graphic card for better performance.	as per the RFP.
45	TPSODL/OT/2021-22/004/5/127	Interfaces : IRIG-B port - 2	We request you to accept GPS based-time facility which supports either NTP or IRIG-B protocol.	as per the RFP.
46	TPSODL/OT/2021-22/004/8/129	Front-end Ports	FCoE protocol is a legacy protocol so majority of storage OEMs does not offer FCoE in their latest storage arrays. Therefore, requesting to remove the requirement of FCoE.	as per the RFP.
47	TPSODL/OT/2021-22/004/8/129	Pt no 6- Storage Capacity & Performance Configured Pt no 8 -Disk Support	Various disk types are required including 300/600 GB 15K RPM disks, 600/900 GB 10K and 1 TB/2 TB/3 TB/4 TB NL-SAS disks. These are old disks and are EOL for supported. Latest storage system support 1.2 TB 10K SAS, 2.4 TB 10K SAS, 6 TB NL-SAS, NL-SAS and 1.92 TB/3.8 TB SSDs. It is requested to alter the requirement accordingly.	Bidders are encouraged to provide latest specification and solution However Minimums Requirement envisaged by customer
48	TPSODL/OT/2021-22/004/8/129	RAID Support	RAID 0 as it does not offer any protection and not offered by majority of storage OEMs. It is requested to modify the clasue as " Should support RAID 1, 10, 5, 6"	as per the RFP.
49	TPSODL/OT/2021-22/004/8/130	Snapshots	copy-on-first-write technique is supported only for a specific vendor so solution is boased to specific OEM. Request to also allow Redirect on Write Technique for Snapshot	as per the RFP.
50	TPSODL/OT/2021-22/004/5/128	Display digit requirements	We request you to modify clause Display Digit height equal or greater than 5.0cm	
51	TPSODL/OT/2021-22/004/9/131	The switch should support auto-sensing 2, 4, 8 Gbps capabilities.	Currently SAN switches are with 16 Gbps will support upto 4 and 8 Gbps. It is requested for deletion of support auto-sensing of 2 Gbps.	as per the RFP.
52	TPSODL/OT/2021-22/004/11/133	Equipment must have one Console port, four or more GbE Ethernet Port, support 75 Gbps or more Firewall throughput and redundant power supply	It is requested to provide details for such high Firewall throughput requirement.	to be discussed during engineering phase
53	TPSODL/OT/2021-22/004/11/133	Network Firewall shall support Layer 3 feature with support for advanced IP Services	Elaborate more details on the required advanced IP services	to be discussed during engineering phase
54	TPSODL/OT/2021-22/004/11/133	Detect and analyse anomalies across network like unexpected connection requests originating from substation for a resources in another substation or Master SCADA DOS events.	Kindly clarify if is there need to provide visibility solution to substations?	to be discussed during engineering phase
55	TPSODL/OT/2021-22/004/11/134	Firewall must have minimum 1 TB HDD for log storage.	Since HDD is older technology than SSD, most of the current applainces comes with SSD based storage as it occupies lesser space. Request to modify the clause as "Firewall must have minimum 400 GB of SSD / 1 TB of HDD for log storage."	Bidders are encouraged to provide latest solution and specification.
56	TPSODL/OT/2021-22/004/11/134	Firewall solution must be field upgradable as per architecture for RAM and ports.	Need more details on upgrade of RAM & interfaces port to size the hardware	to be discussed during engineering phase
57	TPSODL/OT/2021-22/004/Appendix-D/284	BOM	It is requested to add quantities of Control Center Rack Panel, KVM Switch & 17inch Monitor	As we are planning to have all SCADA/DMS servers in TPSODL Data Center, only monotor to be considered.

Sr. No.	Detailed Reference to TPSODL Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
58	TPSODL/OT/2021-22/004/2/48	Multiport Router, IT-OT FW	Kindly confirm that Multiport Router & IT-OT FW1, FW2 will be supplied by TPSODL as given in SCADA/ADMS Architecture	to be discussed during engineering phase
59	TPSODL/OT/2021-22/004/Appendix-D/284	80 Inch TV at Bargarh, Bolangir, Bhawanipatna and BCC	What device it will be connected ? It is requested to share technical specification. How it will be mounted?	This will be display unit and will act as Remote Visual Display. Point should be read as Aska, Bhanjanagar, Rayagada and BCC
60	TPSODL/OT/2021-22/004/Appendix-D/284	SCADA/ ADMS Bill of Material	As per the scope mentioned in the tender document we understand that TPSODL require centralized Main Control Center & Backup Control Center with redundant hardware for all 5 Circles with decentralized remote workstation at 3 Circle. However the quantity provided in SCADA/ ADMS Bill of Material for all the Hardware seems to be very high. We request to clarify the need of such high quantity.	Please refer revised BOM.
61	TPSODL/OT/2021-22/004/Appendix-D/284	Patch Management / Mail / SMS server	The quantity of Patch management server is mentioned 2 numbers at MCC & BCC. Since patch management is non-critical server it is requested to reduce the quantity to 1 number at each location. Patch Management would require internet connection which will be provided by TPSODL. We undersatand existing Mail / SMS server of TPSODL will be integrated with SCADA System kindly confirm the same. We also request to provide server specification for Patch Managent.	**Refer Revised BoM**
62	TPSODL/OT/2021-22/004/Appendix-D/284	B/W Laser printer additional required for Bargarh, Bolangir,and Bhawanipatna Color Laser printer additional required for Bargarh, Bolangir,and Bhawanipatna	There is no technical specification provided for both type of printer. It is requested to provide minimum A4 size technical specification.	Bidder has to provide latest make & model of the printers for black & white and colour. Minimum A4 size.
63	TPSODL/OT/2021-22/004/Appendix-D/284	Storage & Backup Devices	It is requested to ammend 1qty of Tape Library in BOM at MCC & BCC.	**Refer Revised BoM**
64	TPSODL/OT/2021-22/004/Appendix-D/284	Storage & Backup Devices	Since a Tape library (LTO) is already asked for in the specification, all backups are possible using this centralized device which is more suitable for a control room environment than a standalone portable tape unit is not required since it is EOL. Bidder requests the purchaser to delete the requirement of a desktop cartridge magnetic tape unit and its required ports / interfaces in servers and workstations	Bidder has to provide equivalent or better feature & functionality
65	TPSODL/OT/2021-22/004/Appendix-D/284	BOM	Kindly provide soft copy of price schedule for preparation of commercial offer.	ok
66	TPSODL/OT/2021-22/004/Appendix-D/284	Firewall	Kindly confirm the quantity mentioned for firewall in BOM at BCC are in non-redundant configuration.	**Refer Revised BoM**
67	TPSODL/OT/2021-22/004/5.2.2.4 /117	Web servers	Please define the number of concurrent web users	300
68	TPSODL/OT/2021-22/004/2.7/71	System Interfaces	Kindly confirm that ESB is in purchaser scope.	ESB shall be in TPSODL scope.
69	TPSODL/OT/2021-22/004/1.3/46	Scope of Work	Kindly inform the make and version of GIS to be intergated with SCADA/ADMS and provide the sample data of GIS for evaluation.	to be discussed during engineering phase
70	TPSODL/OT/2021-22/004/7.3/14	Delivery Terms	Kindly confirm if Project completion is 800 days or 1090 days as per the defined milestones? Warranty will start after project completion milestone of 1090 days?	Project completion period is 36 months.
71	TPSODL/OT/2021-22/004/2.1.7.1/54	Software Configuration Management	Source code is the intellectual property of the OEM/Supplier. Scorce code shall be provided only for any project specific customizations as per clause 1.3 Scope of work. Kindly confirm.	Source code shall be required by the bidder so that required customization can be done as per the real senerio.
72	TPSODL/OT/2021-22/004/3.6.9/38	Software Minimum Support Period	As per the Standard Industry Practice, the Support period should be total 10 years including warranty. Kindly reconsider.	as per the RFP.
73	TPSODL/OT/2021-22/004/4.6/39	The distribution of marks for experience in implementation of interface is as follows: ⍰ ESB over SOA – 1 marks ⍰ Secured ICCP – 0.5 marks ⍰ CIM (IEC-61968) - 0.5 marks	Purchaser is requested to also accept "Web Services or ESB over SOA " interface to get the marks.	as per the RFP.

Sr. No.	Detailed Reference to TPSODL Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
74	TPSODL/OT/2021-22/004/4.6/39	Project Experience in RTU Implementation (i) IEC 870-5-104 – 0.25 marks (ii) IEC 62056 – 0.25 marks (iii) IEC 61850 – 0.25 marks (iv) IEC 870-5-103- 0.25 marks	IEC 62056 is DLMS protocol relevant for AMI systems and not applicable for SCADA/ADMS IEC 61850 and IEC-103 are substation protocols and RTUs will communicate with substation relays on these protocols and report relevant information to SCADA/ADMS on control center protocols like IEC-104, IEC-101 or DNP3. We request the purchaser to re-evaluate the scoring for this section.	as per the RFP.
75	TPSODL/OT/2021-22/004/4.11.2/108	Display Generation and Editing	From the available specifications it is not clear regarding which changes are required in displays from scripting tool. Since the important information is missing, exact design of solution is not possible before submission. In this regard, it is also requested to restrict the requirement of bulk changes to data modeling. We request to accept the standard tools available in our system.	to be discussed during engineering phase
76	TPSODL/OT/2021-22/004/10.2.10.2b.1/202	Frequency based load shed	The required load shed functionality from control center will not be able to operate fast enough as it will be depending on process time at field and control center, Communication delays etc. It is recommended to operate manual and/or rotational load shed from the control center and perform under-frequency load shed at the local substation level.	to be discussed during engineering phase
77	TPSODL/OT/2021-22/004/8/175	Power system network analysis	Please provide voltage levels considered under Sub transmission network.	33kV and below network shall be considered for power system network analysis.
78	TPSODL/OT/2021-22/004/3.5.8/35	Expendable supplies	Kindly provide more details on the expendable supplies to be considered by supplier with examples.	Bidder has to provide expendable supply based on the overall requirement.
79	TPSODL/OT/2021-22/004/3.6.2/36	Right to change software	SCADA administartors shall be allowed to add, modify or delete database, displays and configuration settings allowed by the SCADA/ADMS software. Kindly confirm is this understanding is in line with the requirements.	as per RFP
80	TPSODL/OT/2021-22/004/11/132	Equipment should have inbuilt support for IPsec VPNs, L2TP & PPTP VPN and it should also support threat free IPsec / L2TP / PPTP VPN. Equipment should support provide SSL-VPN solution with Web Access (Clientless), Full Tunnel and Split Tunnel control. Solution should provide per user / group SSL-VPN access	Request to modify this specification to- "Equipment should have inbuilt support for IPsec VPNs. Equipment should support provide IPSEC and SSL-VPN solution with Full Tunnel and Split Tunnel control. Solution should provide per user / group IPSec and SSL-VPN access" Most browsers (if they haven't already) don't support java anymore - which the java rewriter is the foundation block of clientless feature. Hence Clientless VPN feature is nowadays rarely used and rarely supported. Request to remove that from specification.	Bidder has to provide equivalent or better feature & functionality
81	TPSODL/OT/2021-22/004/11/132	Equipment must have one Console port, four or more GbE Ethernet Port, support 75 Gbps or more Firewall throughput and redundant power supply The proposed integrated IPS should provide 11Gbps or more throughput with 4000+ signature database including the SCADA and other industrial threats. It should support creation of custom IPS signature and creation of multiple IPS policy for different zone.	There is a certain gap of throtughput requirement between Firewall throughput and IPS throughput. Bidder request to modify the Firewall throughput of 30 Gbps or more, and IPS throughput of 10 Gbps or more.	as per the RFP.
82	TPSODL/OT/2021-22/004/11/133	Firewall solution os must not have any vulnerability in OS from last 3 years (till 2018)	Please clarify relevance of the requirement as why the data has been limited to just 2018.	Firewall solution os must not have any vulnerability in OS from last 3 years (till 2020)
83	TPSODL/OT/2021-22/004/11/133	Firewall should support HTTP Request tempering protection, Directory traversal prevention, Form data temering protection, SQL injection Protection, Hidden field manipulation Protection, Session Attacks Mitigation, Banner-grabbing Protection, Buffer overrun Protection, OS command injection Protection, Crosssite scripting Protection (XSS) and Cookie Protections etc.	Some of the mentioned points are very speicific to particular OEM and WAF functionalities- Bidder request to remove WAF specific funcionalities and modify the clause as "Firewall should support HTTP Request tempering protection, Directory traversal prevention, SQL injection Protection, Buffer overrun Protection, OS vulnerability protection, Crosssite scripting Protection (XSS) etc."	Bidder has to provide equivalent or better feature & functionality
84	TPSODL/OT/2021-22/004/8/128	SAN (Storage Area Network) based storage System to have minimum Two controllers, each controller to have 64 bit Quad -core or higher CPU	Bidder request to clarify any specific reason for considering 64GB cache.	to be discussed during engineering phase

Sr. No.	Detailed Reference to TPSODL Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
85	TPSODL/OT/2021-22/004/11/133	Equipment should have inbuilt support for DES, 3DES, AES, Serpent encryption and Pre-shared keys & Digital certificate based authentication connection tunnel.	Request to modify this specification to- "Equipment should have inbuilt support for DES, 3DES, AES and Pre-shared keys & Digital certificate based authentication connection tunnel". Serpent encryption is vendor specific and is not used by customers in real world, bidder request to remove.	Bidder has to provide equivalent or better feature & functionality
86	TPSODL/OT/2021-22/004/11/133	Enabling proactive monitoring and detection of network anamolies covering all industrial protocols like IEC60870-5-101, IEC60870-5-104, IEC61850, DNP3 and TCP/IP	Request to modify the specification as "Enabling proactive monitoring and detection of network anomalies covering all industrial protocols like IEC60870-5-104, DNP3 and TCP/IP etc.".This is vendor specific hence bidder request to remove.	as per the RFP.
87	TPSODL/OT/2021-22/004/7.3/14	The total time for project completion shall not exceed 800 days from the date of placement of firm purchase order by TPSODL.	In project milestone table "Complete of site Acceptance Tests" is shown at 800 days. Does project completion be considered on SAT, please clarify	Project completion period is 36 months.
88	TPSODL/OT/2021-22/004/7.3/14	Delivery schedule	Readiness of infrastucture is not mentioned in the schedule. Shall we assume that the Control Centre is/will be ready in all respect for commissioning Hardware immediately after shipment to site, please clarify	as per the RFP.
89	TPSODL/OT/2021-22/004/7.4/15	Warranty Period 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.	Referring project completion shall not exceed 800 days as mentioned in 7.3, please clarify whether Warranty shall start from SAT completion.	as per the RFP.
90	TPSODL/OT/2021-22/004/3.5/33	Hardware Maintenance The project schedule shall include an allowance for hardware maintenance prior to the availability test (refer to Volume 2, Availability Test). The Supplier will not be granted any relief for project delays caused by maintenance problems prior to the availability test. Maintenance delays during the availability test will be addressed as presented in Volume 2, Availability Test.	Statement not understood. Kindly provide more details on this.	Refer Section 12.11
91	TPSODL/OT/2021-22/004/3.5.3/33	Maintenance during Commissioning Any spare parts found to be defective during initial delivery inspection or during this period shall be replaced within one week after notification.	One week duration is too short for replacement. This is to be changed to 6 weeks minimum	as per the RFP.
92	TPSODL/OT/2021-22/004/3.5.3/33	Failed equipment shall be replaced or repaired and spares inventories (if any) replenished to their delivered level throughout the period of commissioning. Any spare parts found to be defective during initial delivery inspection or during this period shall be replaced within one week after notification. There shall be no charges to TPSODL for these replacement parts, including delivery charges. All spare parts replaced under maintenance shall be new parts unless otherwise accepted by TPSODL's facility.	Please clarify.	Responsibility of failed equipment or spare parts wil be in vendor's responsibility. Any such fault equipment found wil lbe replaced within a week without any additional charge to TPSODL.
93	TPSODL/OT/2021-22/004/1.3/46	Scope of work Study of existing deployed Micro SCADA and migration along with interfaces planned by TPSODL	Please clarify on the 'migration' considered in the scope.	existing DCU/RTU/FRTU will be reporting over IEC 60870-5-104 to MicroSCADA. The migration will be performed by Bidder .
94	TPSODL/OT/2021-22/004/1.3/46	Real time data acquisition from DCU/RTU/FRTU over IEC 60870-5-104 to MCC & BCC	Does existing DCU/RTU/FRTU which will be reporting over IEC 60870-5-104 to MCC & BCC supports Multimaster reporting? Please clarify on changeover from Micro SCADA to New system. Configuration changes required in DCU/RTU/FRTU shall not in scope of bidder	existing DCU/RTU/FRTU will be reporting over IEC 60870-5-104 to Micro SCADA.The migration will be performed by Bidder. RTU/DCU/FRTU configuration not in vendor's scope
95	TPSODL/OT/2021-22/004/1.3/46	Integration with various OT/IT systems like GIS, ERP (SAP), MDM, AMI etc on impending interfaces and provisioning of ESB interface over SOA.	Scope of Coordination with respective vendors of various OT/IT systems is not responsibility of bidder.	Customer will interface with respective vendors for IT systems.

Sr. No.	Detailed Reference to TPSODL Technical Document. Please specify Document No / Clause No / Page No	Description as per Bid Document	Remarks - Query / Clarification	TPSODL Response
96	TPSODL/OT/2021-22/004/14.1.1/259	Providing all SCADA/ADMS equipment and related support materials, including all interconnecting cables and wiring between all Supplier-provided equipment and between the SCADA/ADMS and any equipment furnished by TPSODL site	Please clarify on 'any equipment furnished by TPSODL site'	as per the RFP.
97	TPSODL/OT/2021-22/004/14.1.1/259	Defining the stock of spare parts needed to maintain for system availability	TPSODL considered to provide proper space for storage of spare parts, please confirm.	as per the RFP.
98	TPSODL/OT/2021-22/004/14.1.1/259	Providing an environment that allows for reproducible execution of all SCADA/ADMS functional performance tests conducted during factory acceptance testing	As field equipments are not in the project scope, how the environment will set up to reproduce functional performnce tests. Please clarify.	the Bidder will avail simulator to reproduce actual scenario
99	TPSODL/OT/2021-22/004/14.1.1/259	Verification of existing infrastructure such as the power distribution, air conditioning, power grounding, seismic protection, dust protection, fire protection, equipment size, and other site requirements as necessary for the proper environmental control and operation of all SCADA/ADMS equipment	Verification of the infrastructure shall not be in supplier scope and this shall be excuded from supplier scope.	as per the RFP.
100	TPSODL/OT/2021-22/004/14.1.1/259	Verification of existing infrastructure such as the power distribution, air conditioning, power grounding, seismic protection, dust protection, fire protection, equipment size, and other site requirements as necessary for the proper environmental control and operation of all SCADA/ADMS equipment	Infrastructure related activities like, arrangement of equipments under deliverables shall be in TPSODL scope. Room layout, power and LAN cable routing, interconnection diagrams, location of VPS, Operator WS and server rack shall be in TPSODL scope.	as per the RFP. TPSODLwill provide rack space in its Data Center.
101	TPSODL/OT/2021-22/004/Appendix-D/284	SCADA/ ADMS Bill of Material	Since the Bidder understands that the scope includes combined MCC/BCC control centers for all 5 regions, the quantity for servers in BoQ seems incorrect. Kindly reconfirm the quantities mentioned in the BoQ.	**Refer Revised BoM**

A: - Tentative SCADA /ADMS Revised BoM

S. No.	Equipment		Sambalpur (MCC)	Rourkela (BCC)	total
A	Server/ workstation Hardware with panel	Unit			
1234	**SCADA/ADMS server**	**No.**	**12**	**12**	**24**
	FEP server with interface switches	No.	10	10	**20**
	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 Bargarh, Bolangir,and Bhawanipatna	No.	10	10	**35**
	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 and 80 Inch TV at Bargarh, Bolangir, Bhawanipatna and BCC	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 II switch (SCADA/DMS LAN)-48 ports	No.	8	8	**16**
	Layer II switch (Development system LAN)-24ports additional for Bargarh, Bolangir, Bhawanipatna	No.	4	4	**11**
	Security system (DMZ)				
	Firewall & network IDS/IPS	Nos	4	4	**8**
	Layer II 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 Bargarh, Bolangir,and Bhawanipatna	Set	1	1	**5**
	Color Laser printer additional required for Bargarh, Bolangir,and Bhawanipatna	Set	1	1	**5**
	Cabling System				
	Cable, Jacks etc. additional required for Bargarh, Bolangir,and Bhawanipatna	Lot	1	1	**5**

B	Software for Control Centre				
	SCADA software	Lot	6	6	12
	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 behavior based on the history of the specific resource or metric. These thresholds can vary based on the behavior 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, analyzing, 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 behavior 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

--- END of Document --