ODISHA COMPUTER APPLICATION CENTRE

REQUEST FOR PROPOSAL

Enq.No.:- OCAC-NEGP-INFRA-0007-2021-22061

OCAC invites Request for Proposal (RFP) for selection of Agency for Implementation, Operations and Maintenance of OSWAN NOC. For details please visit websites www.ocac.in & www.odisha.gov.in. **The bid shall be submitted in electronic mode only in the portal https://enivida.odisha.gov.in latest by 13.09.2022, 02:00 PM.** OCAC reserves the right to accept/ reject any/ all bids without assigning any reason thereof.

General Manager(Admin), OCAC, Plot No.-N-1/7-D, Acharya Vihar, P.O.-RRL, Bhubaneswar-751013, Ph.-2567280/ 2567064/ 2567295

Request for Proposal (RFP) for Selection of Agency for Implementation, Operations and Maintenance of OSWAN NOC

RFP Reference No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022

Odisha Computer Application Center

Odisha Computer Application Centre
(Technical Directorate of E&IT Department, Government of Odisha), N-1/7-D, Acharya Vihar, PO- RRL, Bhubaneswar – 751013
EPBX: 0674 -2567280 / 2567064 /2567295 / 2567283

DISCLAIMER

The information contained in this RFP document or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by Odisha Computer Application Centre(OCAC) or any of their employees is provided to Bidder(s) on the terms and conditions set out in this RFP Document and such other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is neither an offer nor invitation by OCAC to the Bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in making their technical and financial offers pursuant to this RFP (the "Bid"). This RFP includes statements, which reflect various assumptions and assessments arrived at by the bidder in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. The assumptions, assessments, statements and information contained in this RFP, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigations, studies and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP and obtains independent advice from appropriate sources.

Information provided in this RFP to the Bidder(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

OCAC, makes no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Bid Stage. OCAC also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.

OCAC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP. The issue of this RFP does not imply that is bound to select a Bidder or to appoint the Preferred Bidder, as the case may be, for the Project and reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.
OCAC reserves all the rights to cancel, terminate, change or modify this selection process and/or requirements of bidding stated in the RFP, at any time without assigning any reason or providing any notice and without accepting any liability for the same.

Table of Contents

1. Important Dates & Information

Information	Details
Bid Inviting Authority	Odisha Computer Application Centre (OCAC) (Technical Directorate of I.T. Dept, Govt. of Odisha)
Correspondence Address	The General Manager (Admin), Odisha Computer Application Centre (OCAC), (Technical Directorate of I.T. Dept, Govt. of Odisha), N-1/7-D, Acharya Vihar, P.O.- RRL, Bhubaneswar – 751013
RFP Name	Request for Proposal (RFP) for Implementation, Operations and Maintenance of OSWAN NOC.
Bid Reference No. and Date	OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022
Place of Execution	Odisha Computer Application Centre (OCAC), (Technical Directorate of I.T. Dept, Govt. of Odisha), N-1/7-D, Acharya Vihar, P.O.- RRL, Bhubaneswar – 751013
Non-Refundable RFP Document Fee	₹22,400/- (Rupees Twenty Two Thousand Four Hundred Only), (Inclusive of 12% GST) in the form of Demand Draft drawn from any Scheduled Bank in favour of "Odisha Computer Application Centre", payable at Bhubaneswar or paid online through OCAC e-Tender Portal, i.e., https://enivida.odisha.gov.in/
EMD	Bid Security Declaration Form as per ***Annexure - 3***
Availability of Bid Document in the website(www.ocac.in, www.odisha.gov.in & https://enivida.odisha.gov.in)	23.08.2022
Last Date and Time for Submission of Pre-Bid Query through email only	30.08.2022 by 02:00 PM
Date & Time for Pre-Bid Conference through online VC	02.09.2022, 02:00 PM
Issue of Corrigendum (if any)	06.09.2022
Last Date and Time for Submission of Bid Document	**13.09.2022 at 02:00 PM**
Date and Time of opening of Pre-Qualification Bids	13.09.2022 at 04:00 PM
Date and Time of opening of Technical Bids	To be informed
Opening of Commercial Bid (CB)	To be informed

1.1. Fact Sheet

This Fact Sheet comprising important factual data of the tender is for quick reference of the Bidder.

Clause Reference	Topic
The Proposal	Odisha Computer Application Centre (OCAC) invites RFP for selection of agency for Implementation, Operations and Maintenance of OSWAN NOC.
Method of Selection	Least cost-based method (L1) shall be used to select the Bidder. The Bidder has to submit the bid online through https://enivida.odisha.gov.in/
RFP Document Fee	RFP Document fee Rs.22,400/- (Rupees Twenty Two Thousand Four Hundred Only), (Inclusive of 12% GST) must be submitted along with the proposal. The RFP document fee must be in favor of Odisha Computer Application Centre from any Scheduled Bank payable at Bhubaneswar or paid online through https://enivida.odisha.gov.in/.
Earnest Money Deposit (EMD)	Bid Security Declaration Form as per ***Annexure - 3***
Performance Bank Guarantee (PBG)	Performance Bank Guarantee (PBG) @ 3% of the cost of project from any Scheduled Bank in the prescribed format in favour of the Odisha Computer Application Centre shall be submitted by the successful bidder within 15 **days** of issue of work order.
Scope of Work	Selected bidder is expected to deliver the services listed in Scope of Work as mentioned in this RFP
Language	Bid must be prepared by the bidder in English language only
Currency	The bidder should quote in Indian Rupees only. The Total Price inclusive of taxes and duties will be considered for evaluation. So, the bidder must mention the base price and the tax component separately.
Validity Period	Proposals/bid must remain valid minimum for 180 days from the last date of bid submission.
Bid to be submitted on or before last date of submission at:	The proposal must be submitted to: **The General Manager (Admn.)** Odisha Computer Application Centre (OCAC) OCAC Building, Plot No.-N-1/7-D, Acharya Vihar Square, RRL Post Office, Bhubaneswar-751013 (INDIA)

1.2. Abbreviation

Abbreviations	Description
BDF	Bid Declaration Form
NIA	NOC Implementing Agency
NOC	Network Operations Centre
OCAC	Odisha Computer Application Centre
EMS	Element Management System
NMS	Network Management System
OSWAN	Odisha State Wide Area Network
EMD	Earnest Money Deposit
RFP	Request for Proposal
TPA	Third Party Agency
OEM	Original Equipment Manufacturer
FAT	Final Acceptance Test
PAT	Partial Acceptance Test

2. Invitation for Bids

Odisha Computer Application Centre (OCAC) invites bids from eligible bidders who have the necessary qualifications for Implementation, Operations and Maintenance of OSWAN NOC as per the “Scope of Work” described in this RFP. The Agency shall be responsible for implementing the OSWAN-NOC and providing the operations and maintenance support for 5 years from the date of FAT.

The Bid document has been published in the official website of OCAC (www.ocac.in), OCAC e-Tender Portal https://enivida.odisha.gov.in and official website of Govt. of Odisha (www.odisha.gov.in). The tender advertisement has also been published in leading newspapers for wide circulation. Bidders are requested to go through the Bid document carefully and participate in the bidding process with all necessary details as required.

This RFP is issued by OCAC, which is the sole point of contact during the selection process. The Nodal Officer responsible for entire process is General Manager (Admin).

3. Background Information

State Wide Area Network Project aims at establishment of Wide Area Network connectivity for G2G functioning, up to Block Level. State Wide Area Network (SWAN) is one of the flagship programs under Core Infrastructure Projects of NeGP. The main purpose of this network is to create a dedicated Closed User Group (CUG) network and provide secured and high speed connectivity for Government functioning and connecting State Headquarters, District Headquarters and Block Headquarters. SWAN basically intends to focus on the Govt. to Govt. (G2G) functions.

Odisha is amongst the primary states where SWAN is successfully implemented and operational since 2010. Under the SWAN Project, total no of PoPs identified are 1605. The detailed classification of PoPs is mentioned below:

PoPs under ODISHA STATE WIDE AREA NETWORK	
SHQ	01
DHQ	30
BHQ	314
Old Horizontal Offices	47
New Horizontal Offices	1191
Total	**1583**

3.1. Basic Information:

OSWAN has been envisaged at the state level primarily to connect various departments and enable effective and efficient transmission of information within the state so that the financial and social benefits that could be derived via the utilization of an IT enabled platform could be availed optimally. OSWAN acts as a primary vehicle effective communication of voice, data and video throughout the state and is an effective tool for service delivery by Government Institutions.

Odisha Computer Application Centre (OCAC) has been designated as the state level Nodal Agency for finalizing the procurement process for engagement Bandwidth Service Provider, Network Service Provider and Third party Auditor for Odisha SWAN implementation. Odisha SWAN was implemented and made operation keeping in view the Govt.'s intension to link government offices at state headquarters (SHQ) at Bhubaneswar; all district headquarters (DHQ), and all Block headquarters (BHQ), all Horizontal Offices (HO), with each other at each of these locations. OSWAN was implemented on Build-Own-Operate and Transfer (BOOT) basis to provide data, voice and video services to various offices of Govt. of Odisha and other locations as identified by OCAC. The OSWAN possesses suitable topology, use state-of-the art technologies and have capability and flexibility to expand and upgrade to cover all parts of the state. The Implementation was carried out in phases. In Phase-1 the offices which were included are SHQ, 30 DHQs and 279 BHQs, in Phase – 2, rest 35 BHQs and 47 Horizontal offices and in Phase – 3, 1213 new Horizontal offices, have been taken for implementation. BSNL has provided MPLS connectivity in all DHQs, BHQs & 347 HOs and conventional Leased Line (Point to Point) connectivity in rest of the PoPs to establish the Odisha State Wide Area Network. Odisha SWAN in implemented in a Three Tier network Architecture. The detailed bandwidth distribution across all PoPs under existing OSWAN along with the existing Network Architecture is elaborated in subsequent sections of this RFP.

Existing Connectivity in Odisha SWAN					
SL#	**Name of the PoP**	**Qty**	**Bandwidth**	**Type of Connectivity**	**Name of the ISP**
1.	SHQ	1	2 Gbps	MPLS	BSNL
		1	1 Gbps	P2P	NKN
		1	1 Gbps	ILL	RailTel
2.	DHQ	30	16 Mbps	MPLS	BSNL
3.	BHQ	314	8 Mbps	MPLS	BSNL
4.	HO (Tehesil)	317	4 Mbps	MPLS	BSNL
5.	HO (DRDA)	30	4 Mbps	MPLS	BSNL
6.	Old HO	47	2 Mbps	P2P Lease Line	BSNL
7.	New HO	844	2 Mbps	P2P Lease Line	BSNL

This RFP is issued by OCAC, which is the sole point of contact during selection process. The officer responsible for entire process is **General Manager (Admin)**. The purpose of this RFP is to provide interested Bidder with information to enable them to prepare and submit a proposal for Implementation, Operations and Maintenance of OSWAN NOC for Odisha State Wide Area Network infrastructure.

4. Pre-Qualification/Eligibility Criteria

Following table describe the pre-qualification criteria. A bidder participating in the bidding process shall possess the following minimum pre-qualification/ eligibility criteria. Any bidder failing to meet the stated criteria shall be summarily rejected and will not be considered for Technical Evaluation.

Sl. No.	PQ Criteria	Description of the Criteria	Documents to be Submitted
1.	**General**	The Bidder or its OEM incorporated or any OEM Product manufactured in a country sharing a land boundary with India cannot participate in this bid.	Declaration by the Bidder / OEM on their letter head in this regard should submit along with the Bid.
2.	**Legal Entity**	The bidder must be a company registered in India under Indian Companies Act 1956 and 2013 OR A Partnership firm registered under Indian Partnership Act, 1932, The bidder must be in operation since last 3 years as on 31st March 2022. The bidder must have GST registration & up-to-date Income Tax Return, PAN Number as on 31st March 2021.	a. Valid copy of certificate of incorporation and registration certificates. b. Copy of GST registration. c. Copies of relevant Certificates of registration Income Tax / PAN Number from the respective Government Department.
3.	**Turnover**	The average annual turnover of the bidder during the last three financial year ending with 31st March 2021 should not be less than ₹ 70 crore from IT/ITeS (as per the last published audited balance sheets / CA certified provisional balance sheet).	- Audited Balance Sheets - Valid CA Certificate.
4.	**Net Worth**	The net worth of the bidder in	- Valid CA Certificate

		the last three financial year ending on 31st March 2021, (as per the last published audited balance sheet / CA certified provisional balance sheet) should be Positive.	
5.	**Technical Capability**	The bidder must have successfully undertaken at least the following numbers of similar assignments, in last five years, of value specified herein: - One project of similar nature in system integration, not less than the amount ₹17,00,00,000/- (Seventeen Crore Only) **OR** - Two projects of similar nature in system integration, not less than the amount ₹13,00,00,000/- (Thirteen Crore Only) **OR** -Three project of similar nature in system integration, not less than the amount of ₹9,00,00,000/- (Nine Crore Only) **"Similar Nature" is defined as: Implementation, Operation & Maintenance of Network Operation Centre or Data Centre (Must be included IT & Non-IT Components) or any project having Network Operation Centre or Data Centre (Must be included IT & Non-IT Components) Government / Semi Government/ PSU/ BFSI Sector**	Satisfactory Work completion certificates from the client +Copy of the Work Order **OR** Copy of Work Order +Self-Certificate of satisfactory work completion certificate/work in progress (Certified by the Statutory Auditor) **OR** Copy of Work Order + Phase Completion Certificate from the client for ongoing projects.

		in India.	
6.	**Quality Certification**	The bidder must possess a valid ISO 9001, ISO20000, ISO 27000 Certification	Copies of the valid certificates.
7.	**Blacklisting**	The bidder should not be under a declaration of ineligibility for corrupt and fraudulent practices issued by any Government/PSU/BFSI Sector in India.	Self- declaration
8.	**OEM Authorization**	The bidder must attach Manufactures Authorization certificate specific to this tender & Back-to-back support letter from OEMs for providing Comprehensive support and services of the OEM's product covered under the RFP.	OEM MAF
9.	**Local Presence**	The bidder should have an office in Odisha. However, if the presence is not there in the state, the bidder should give an undertaking for establishment of an office, within one month of award of the contract.	Relevant Documents supporting office addresses/ Undertaking.
10.	**Document Fee**	The bidder must have made a payment of ₹22,400.00 (Rupees Twenty Two Thousand Four Hundred Only) towards tender document fee.	The RFP document fee must be paid online through https://enivida.odisha.gov.in/
11.	**EMD**	Bid Security Declaration Form	Annexure - 3

5. Instruction to Bidders

5.1. General

a) While every effort has been made to provide comprehensive and accurate background information and requirements and specifications, Bidders must form their own conclusions about the solution needed to meet the requirements. Bidders and recipients of this RFP may consult their own legal advisers with regard to this RFP.

b) All information supplied by Bidders may be treated as contractually binding on the Bidders, on successful award of the assignment by OCAC on the basis of this RFP.

c) No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of the OCAC. Any notification of preferred bidder status by OCAC shall not give rise to any enforceable rights by the Bidder. OCAC may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of the OCAC.

d) This RFP supersedes and replaces any previous public documentation & communications, and Bidders should place no reliance on such communications.

5.2. Availability of RFP Document

a) The availability of bidding documents shall be commenced from the date as mentioned in Notice Inviting Bids (NIB). The complete bidding document can be downloaded from the official website of OCAC (www.ocac.in), e-Tender Portal of OCAC (https://enivida.odisha.gov.in) and Official website of Govt. of Odisha (www.odishsa.gov.in). The prospective bidders are requested download the bidding document from the websites and follow the bidding steps as prescribed.

b) The bid Notice is also published in leading newspapers (Odia & English) for wide Circulation.

5.3. Compliant Proposals/ Completeness of Response

a) Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

b) Failure to comply with the requirements set out in this RFP may render the Proposal noncompliant and the Proposal may be rejected. Bidders must include all documentation specified in this RFP.
c) Follow the format and respond to each element in the order as set out in this RFP. Comply with all requirements as set out within this RFP.

5.4. Period of Validity of Bids

a) Bids submitted by the bidders shall remain valid for a period of 180 Days from the date of submission of RFP.

b) Prior to the expiry of the period of validity of Bids, the procuring entity, in exceptional circumstances, may request the bidders to extend the bid validity period for an additional specified period. A bidder may refuse the request and such refusal shall be treated as withdrawal of Bid and in such circumstances bid security shall not be forfeited.

c) Bidders who agree to an extension of the period of validity of their Bids shall extend or get extended the period of validity of bid securities submitted by them or submit new bid securities to cover the extended period of validity of their bids. A bidder whose bid security is not extended, or that has not submitted a new bid security, is considered to have refused the request to extend the period of validity of its Bid.

5.5. Right to Accept Any Proposal and To Reject Any or All Proposal(s)

a) OCAC reserves the right to accept or reject any proposal at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for such action.

b) OCAC makes no commitments, express or implied, that this process will result in a business transaction with anyone.

c) The submission of RFP does not constitute an offer by OCAC. The bidder's participation in this process may result in selecting the bidder to engage towards execution of the contract.

5.6. Format and Signing of Bids

a) All the Bids submitted by the bidders must be submitted with the checklist.
b) Each page of the bidding document shall be kept with the office seal and signature by the authorized representative from the Bidder.

5.7. Cost & Language of Bidding

a) The bidder shall be responsible for all costs incurred in connection with participation in the bid process, including site visits but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/ discussions / presentations, preparation of bid, in providing any additional information required by OCAC to facilitate the evaluation process, and in negotiating a definitive contract or all such activities related to the bid process. OCAC will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

b) The Proposal should be filled by the Bidder in English language only. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the Bidders. For purposes of interpretation of the Proposal, the English translation shall govern.

5.8. Alternative/ Multiple Bids

a) Each bidder shall submit only one Proposal. The bidder who submits more than one proposal will be disqualified.

b) The bidders are not allowed to quote for multiple brands / make/ model for item in the Technical Bid and should also mention the details of the quoted make/ model of the respective items.

5.9. RFP Document Fees

The bidders are required to pay the RFP Document Fee of ₹22,400/-(inclusive of 12% GST), online through e-Tender Portal (https://enivida.odisha.gov.in/). Proposals received without or with inadequate RFP Document fees shall be rejected.

5.10. Earnest Money Deposit (EMD)/BID Security

a. Bidders shall submit, Bid Declaration Form (BDF) at Annexure – 3. The BDF should be submitted in the General/Pre-qualification Bid.
b. The bid / proposal submitted without BDF, mentioned above, will be summarily rejected.

5.11. Pre-Bid Meeting & Clarifications

a) Bidders are requested to submit their queries by e-mail to gm_ocac@ocac.in and orissaswan@gmail.com as per the format (***Annexure-13***) given in RFP on or before 30.08.2022, 02:00 PM.

b) A pre-bid conference will be scheduled by OCAC to clarify doubts of potential bidders in respect of the procurement and the records of such conference shall be published on the respective websites as Pre-bid clarifications.

c) The Pre-Bid Conference will be held through Video Conferencing. The link for VC will be shared with participants before schedule. The details of the prebid meeting schedule is mentioned in "Important Dates and information" section of this RFP.

d) Prospective bidders, who have deposited the prescribed tender fee to the OCAC as specified in RFP, are allowed to attend the pre-bid conference/ meeting and their query will be addressed.

5.12. Responses to Pre-Bid Queries and Issue of Corrigendum

a) The Nodal Officer mentioned in the RFP document will endeavour to provide timely response to all queries. However, OCAC makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does OCAC undertake to answer all the queries that have been posed by the applicants. The responses to the queries from all applicants will be published on OCAC website.

b) At any time prior to the last date for receipt of RFP, OCAC may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective applicant, modify the RFP Document by a corrigendum.

c) The Corrigendum (if any) & clarifications to the queries from all applicants will be published by OCAC on the website.

d) Any such corrigendum shall be deemed to be incorporated into this RFP.

e) In order to provide prospective applicants reasonable time for taking the corrigendum into account, OCAC may, at its discretion, extend the last date for the receipt of RFP.

5.13. Submission of Proposals

5.13.1. Instruction to Bidders for Online Bid Submission

e-Nivida is a complete process of e-Tendering, from publishing of Tenders online, inviting online bids, evaluation and award of contract using the system. The instructions given below are meant to assist the bidders in registering on e-Nivida Portal and submitting their bid online on the portal. More information useful for submitting online bids on the e-Nivida Portal may be obtained at: https://enivida.odisha.gov.in.

5.13.2. Guidelines for Registration

a) Bidders are required to enrol themselves on the eNivida Portal https://enivida.odisha.gov.in or click on the link “Bidder Enrolment” available on the home page by paying Registration Fees of Rs.5,600/- inclusive of Applicable GST.

b) As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.

c) Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication with the bidders.

d) Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Only Class III Certificates with signing + encryption key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify/ TCS / nCode/ eMudhra etc.), with their profile.

e) Only valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSC’s to others which may lead to misuse.

f) Bidder then logs in to the site through the secured log-in by entering their user ID /password and the password of the DSC / e-Token.

g) The scanned copies of all original documents should be uploaded in pdf format on e-Tender portal.

h) After completion of registration payment, bidders need to send their acknowledgement copy on our help desk mail id odishaenivida@gmail.com for activation of the account.

5.13.3. Searching for Tender Documents

a) There are various search options built in the e-Tender Portal, to facilitate bidders to search active Tenders by several parameters.

b) Once the bidders have selected the Tenders they are interested in, then they can pay the Tender fee and processing fee (NOT REFUNDABLE) by net-banking / Debit / Credit card then you may download the required documents / Tender schedules, Bid documents etc. Once you pay both fee Tenders will be moved to the respective 'requested' Tab. This would enable the e- Tender Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the Tender document.

5.13.4. Preparation of Bids

a) Bidder should take into account any corrigendum published on the Tender document before submitting their bids.

b) Please go through the Tender advertisement and the Tender document carefully to understand the documents required to be submitted as part of the bid.

c) Bidder, in advance, should get ready the bid documents to be submitted as indicated in the Tender document / schedule and generally, they can be in PDF formats. Bid Original documents may be scanned with 100 dpi with Colour option which helps in reducing size of the scanned document.

d) To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, GST, Annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use "My Documents" available to them to upload such documents.

e) These documents may be directly submitted from the "My Documents" area while submitting a bid and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process. Already uploaded documents in this section will be displayed. Click "New" to upload new documents.

5.13.5. Submission of Bids

a) Bidder should log into the website well in advance for the submission of the bid so that it gets uploaded well in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.

b) The bidder has to digitally sign and upload the required bid documents one by one as indicated in the Tender document as a token of acceptance of the terms and conditions laid down by Department.

c) Bidder has to select the payment option as per the Tender document to pay the Tender fee / Tender Processing fee & EMD as applicable and enter details of the instrument.

d) In case of BG bidder should prepare the BG as per the instructions specified in the Tender document. The BG in original should be posted/couriered/given in person to the concerned official before the Online Opening of Financial Bid. In case of non-receipt of BG amount in original by the said time, the uploaded bid will be summarily rejected.

e) Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BOM format with the Tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BOM file, open it and complete the yellow Coloured (unprotected) cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BOM file is found to be modified by the bidder, the bid will be rejected.

f) The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.

g) The uploaded bid documents become readable only after the Tender opening by the authorized bid openers.

h) Upon the successful and timely submission of bid click "Complete" (i.e. after Clicking "Submit" in the portal), the portal will give a successful Tender submission

acknowledgement & a bid summary will be displayed with the unique id and date & time of submission of the bid with all other relevant details.

i) The Tender summary has to be printed and kept as an acknowledgement of the submission of the Tender. This acknowledgement may be used as an entry pass for any bid opening meetings.

5.13.6. Clarifications on using e-Nivida Portal

a) Any queries relating to the Tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a Tender or the relevant contact person indicated in the Tender.

b) Any queries relating to the process of online bid submission or queries relating to e-Tender Portal in general may be directed to the Helpdesk Support. Please feel free to contact e-Nivida Helpdesk (as given below) for any query related to e-Tendering.

Phone No.: 011-49606060

Mail id: odishaenivida@gmail.com

5.14. Submission of Manufacturer's Authorization Form

Bidder must submit the duly signed MAF at the time of bid submission in the Prequalification Proposal as per the prescribed format (Annexure-6). The MAF should be submitted in OEM's letter head mentioning required details. Also OEM's should confirm the Bidder's participation to OCAC.

5.15. Deadline Submission of Bids

a) Bidder must ensure to submit their response on or before the deadline date as mentioned in "Important Dates & Information" section of this RFP.

b) Normally, the date of submission and opening of Bids will not be extended. In exceptional circumstances or when the bidding document are required to be substantially modified as a result of discussions in pre-bid meeting/ conference or otherwise and the time with the prospective bidders for preparation of Bids appears insufficient, the date may be extended by the procuring entity. In such case the publicity of extended time and date shall be given in the manner, as was given at the time of issuing the original Bidding Document.

c) It shall be ensured that after issue of corrigendum, reasonable time is available to the bidders for preparation and submission of their Bids. OCAC shall also publish such modifications in the bidding document in the same manner as the publication of initial bidding document. If the last date of submission or opening of Bids is a non- working day, the Bids shall be received or opened on the next working day.

5.16. Venue for Submission of Bids

Response to Bid, in its complete form in all respects as specified in the RFP, must be submitted to OCAC at the address specified below:

Address To	General Manager(Admin) Odisha Computer Application Centre N-1/7-D, Acharya Vihar Square, PO: RRL Bhubaneswar – 751002 Odisha
Telephone	0674-2567280/ 2567064/ 2567295
Fax	0674-2567842
Email id	gm_ocac@ocac.in

5.17. Withdrawal, Substitution, and Modification of Bids

a) If permitted by OCAC, a Bidder may withdraw its Bid or re-submit its Bid as per the instructions/ procedure prescribed by OCAC.

b) Bids withdrawn shall not be opened and processed further.

5.18. Opening of Bids

a) The Bids shall be opened by the Proposal Evaluation Committee in the presence of the bidders or their authorised representatives who choose to be present.

b) The committee may co-opt experienced persons in the committee to conduct the process of Bid opening.

c) The committee shall prepare a list of the bidders or their representatives attending the opening of Bids and obtain their signatures on the same. The list shall also contain the representative's name and telephone number and corresponding bidders' names and addresses. The authority letters, if any, brought by the representatives shall be attached to the list. The list shall be signed by all the members of Bid opening committee with date and time of opening of the Bids.

d) The committee shall conduct a preliminary scrutiny of the opened technical Bids to assess the prima-facie responsiveness and ensure that the: -
   i. Bid is accompanied by bidding document fee, bid security or bid securing declaration, and processing fee (if applicable).
   ii. Bid is valid for the period, specified in the bidding document.

iii. Bid is unconditional and the bidder has agreed to give the required performance security and other conditions, as specified in the bidding document are fulfilled.

iv. Any other information which the committee may consider appropriate.

e) No Bid shall be rejected at the time of Bid opening except the Bids not accompanied with the proof of payment or instrument of the required price of bidding document, processing fee and bid security.

f) The Financial Bid cover shall be kept unopened and shall be opened later on the date and time intimated to the bidders who qualify in the evaluation of technical Bids.

5.19. RFP Evaluation

5.19.1. Evaluation & Tabulation of Pre-Qualification Bid

a) Determination of Responsiveness: The designated committee of OCAC shall determine the responsiveness of a Bid on the basis of bidding document and the provisions of pre-qualification/ eligibility criteria of the bidding document.

b) A responsive Bid is one that meets the requirements of the bidding document without any material deviation, reservation, or omission where: -

1. “Deviation” is a departure from the requirements specified in the bidding document.
2. “reservation” is the setting of limiting conditions or withholding from complete acceptance of the requirements specified in the bidding document; and
3. “Omission” is the failure to submit part or all the information or documentation required in the bidding document.

c) A material deviation, reservation, or omission is one that, if accepted, shall: -

1. affect in any substantial way the scope, quality, or performance of the subject matter of procurement specified in the bidding documents; or
2. limits in any substantial way, inconsistent with the bidding documents, the procuring entity’s rights or the bidder’s obligations under the proposed contract, OR
3. If rectified, shall unfairly affect the competitive position of other bidders presenting responsive Bids.

d) The designated committee of OCAC shall examine the technical aspects of the Bid in particular, to confirm that all requirements of bidding document have been met without any material deviation, reservation or omission.

e) Fulfilment of eligibility criteria: All the criteria mentioned in **Clause No-4 (Pre-Qualification/Eligibility Criteria)** are mandatory. The bidder must comply with all the components mentioned in the eligibility criteria.

f) All supporting documents as mentioned in **Annexure-14.**

5.19.2. Evaluation & Tabulation of Technical Bids

Technical Bids of the Bidders, who qualified in the Pre-Qualification Criteria, will be considered for further evaluation. The Technical evaluation committee will evaluate the technical response submitted by the Bidder. The Technical bid response includes the below details:-

a) The Technical Bid response will be initiated with the Technical Bid Cover letter in specified format as mentioned in **Annexure-5.**
b) Detailed Compliance Sheet of the Technical Specification dully signed in Company Letter Head /OEM's Letter Head.
c) Detailed Bill of material keeping in view the Requirement including all appliances, licenses, accessories and others proposed as per **Annexure -11.**
d) In case of deviation while evaluating the Technical Bid response based upon the criteria, the bid will be subjected for rejection.
e) All supporting documents as mentioned in **Annexure-14.**

5.19.3. Evaluation & Tabulation of Financial Bids

a) The financial bids/ cover of the bidders who qualify in pre-qualification/eligibility criteria shall be opened at the notified time, date and place by the members of the designated Procurement Committee in the presence of the bidders or their representatives who choose to be present.

b) The financial bid cover letter should be submitted in appropriate format as per **Annexure-7** followed by financial bid details as per **Annexure-12.**

c) The process of opening of financial bids/ covers shall be similar to that of technical bids.

d) The names of the bidders, the rates given by them and conditions put, if any, shall be read out and recorded.

e) Only fixed price financial bids indicating total price for all the deliverables and services specified in this bid document will be considered.

f) Prices quoted in the Bid must be firm and final and shall not be subject to any modifications, on any account whatsoever except applicable tax rates. The Bid Prices shall be indicated in Indian Rupees (INR) only.

g) The bid price will include all taxes and levies and mentioned separately.
h) Any conditional bid would be rejected.

i) If there is no price quoted for certain material or service, the bid shall be declared as disqualified.

j) Commercial bids of those Bidders who are technically qualified in the technical evaluation will only be opened. All other commercial bids will not be opened. The financial evaluation shall be done based on the details submitted by the bidder as per the format provided. The bidders shall be sorted in the ascending order as L1, L2, and L3 etc.

k) L1 bidder will be selected for award of contract, after final evaluation.

5.19.4. Correction of Arithmetic Errors in Financial Bids

The Proposal evaluation committee shall correct arithmetical errors in substantially responsive Bids, on the following basis, namely: -

a) If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected, unless in the opinion of the Proposal Evaluation Committee there is an obvious misplacement of the decimal point in the unit price, in which case the total price as quoted shall govern and the unit price shall be corrected.

b) If there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected; and

c) If there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to clause (a) and (b) above.

5.20. Exclusion of Bids / Disqualification

a) A procuring entity shall exclude/ disqualify a Bid, if: -

   i. The information submitted, concerning the qualifications of the bidder, was false or constituted a misrepresentation; or

   ii. The information submitted, concerning the qualifications of the bidder, was materially inaccurate or incomplete; and

   iii. The bidder is not qualified as per pre-qualification/ eligibility criteria mentioned in the bidding document.

   iv. The Bid materially departs from the requirements specified in the bidding document or it contains false information.

   v. The bidder, submitting the Bid, his agent or any one acting on his behalf, gave or agreed to give, to any officer or employee of the procuring entity or other governmental authority a gratification in any form, or any other thing of value, so as to unduly influence the procurement process;

vi. A bidder, in the opinion of the procuring entity, has a conflict of interest materially affecting fair competition.

b) Bid shall be excluded/ disqualified as soon as the cause for its exclusion / disqualification is discovered.

c) Every decision of a procuring entity to exclude a Bid shall be for reasons to be recorded in writing and shall be: -

i. Communicated to the concerned bidder in writing.

ii. Published on the State Public Procurement Portal, if applicable.

5.21. Lack of Competition

a) A situation may arise where, if after evaluation of Bids, the proposal evaluation committee may end-up with one responsive Bid only. In such situation, the Proposal Evaluation Committee would check as to whether while floating the Bid all necessary requirements to encourage competition like standard bid conditions, industry friendly specifications, wide publicity, sufficient time for formulation of Bids, etc. were fulfilled. If not, the tender would be re-floated after rectifying deficiencies. The bid process shall be considered valid even if there is one responsive Bid, provided that: -

i. The Bid is technically qualified.

ii. The price quoted by the bidder is assessed to be reasonable.

iii. The Bid is unconditional and complete in all respects.

iv. There are no obvious indicators of cartelization amongst bidders; and

v. The bidder is qualified as per the provisions of pre-qualification/ eligibility criteria in the bidding document.

b) The Proposal Evaluation Committee shall prepare a justification note for approval by the next higher authority of the procuring entity, with the concurrence of the account's member.

c) In case of dissent by any member of Proposal Evaluation Committee, the next higher authority in delegation of financial powers shall decide as to whether to sanction the single Bid or re-invite Bids after recording reasons.

5.22. Acceptance of the successful Bid and award of Project

5.22.1. Award Criteria

OCAC will award the Project to the successful bidder whose proposal has been determined to be substantially responsive and has been determined as the most responsive bids as per the process outlined above.

5.22.2. Purchaser's Procurement Rights

Without incurring any liability, whatsoever to the affected bidder or bidders, the Purchaser reserves the right to: -

a) Amend, modify, or cancel this tender and to reject any or all proposals without assigning any reason.
b) Change any of the scheduled dates stated in this tender.
c) Reject proposals that fail to meet the tender requirements.
d) Increase or decrease the quantity of the items at the time of placement of order.
e) Increase or decrease no. of resources supplied under this project.
f) Make typographical correction or correct computational errors to proposals
g) Request bidders to clarify their proposal.

5.22.3. Notification of Award

Prior to the expiry of the validity period, OCAC will notify the successful bidder in writing or by fax or email, that its proposal has been accepted. In case the tendering process / public procurement process has not been completed within the stipulated period, OCAC may like to request the bidders to extend the validity period of the bid. The notification of award will constitute the formation of the contract. Upon the successful bidder's furnishing of Performance Bank Guarantee, OCAC will notify each unsuccessful bidder and return their EMD.

5.22.4. Issuance of Purchase Order

a. The OCAC shall reserve the right to negotiate with the bidder(s) whose proposal has been ranked best value bid on the basis of Technical and Commercial Evaluation to the proposed Project, as per the guidance provided by CVC. On this basis the Purchase order would be issued.
b. The bidder has to give its acceptance within 7 days of Issuance of Purchase Order. In case OCAC has not received the acceptance or the selected bidder will refuse to accept the Purchase Order, OCAC may intimate the next competitive bidder to award the Purchase Order.

5.22.5. Performance Guarantee

The OCAC will require the Agency to provide a Performance Bank Guarantee, within 15 days from the Notification of award, for a value equivalent to 3% of the total cost of ownership i.e. total order value excluding taxes. The Performance Guarantee should be valid till Entire Project Period of 5 years 3 months (63 months). However the Bidder may submit PBG for a period of 3 Years 3 months (39 months) & subsequently renewed for another 2 years before expiry else the PBG will be forfeited. The Performance Guarantee shall be kept valid till completion of the project and support period. The Agency shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the project and support period. In case the Agency fails to submit performance guarantee within the time stipulated, the OCAC at its discretion may cancel the order placed on the

Agency after giving prior written notice to rectify the same. OCAC shall invoke the performance guarantee in case the selected Bidder fails to discharge their contractual obligations during the period or OCAC incurs any damages due to Bidder's negligence in carrying out the project implementation as per the agreed terms & conditions.

5.22.6. Signing of Contract

After the OCAC notifies the successful bidder that its proposal has been accepted, OCAC shall enter into a contract within thirty (30) days of the award of the contract or within such extended period, as may be specified by the Authorized Representative of OCAC., incorporating all clauses and the proposal of the bidder with the successful bidder. The Draft Service Level Agreement (SLA) will be provided as a separate document.

5.22.7. Failure to Agree with the Terms and Conditions of the RFP

Failure of the successful bidder to agree with the Terms & Conditions of the RFP and the Proposal submitted by the successful bidder, despite the deviations submitted by the Bidder are adequately considered and mutually agreed, shall constitute sufficient grounds for the annulment of the award, in which event OCAC may award the Project to the next best value bidder or call for new proposals from the interested bidders. In such a case, the OCAC shall invoke the PBG or the EMD as the case may be, of the most responsive bidder.

5.23. Confidentiality

a) Notwithstanding anything contained in this bidding document but subject to the provisions of any other law for the time being in force providing for disclosure of information, a procuring entity shall not disclose any information if such disclosure, in its opinion, is likely to: -
   i. Impede enforcement of any law.
   ii. Affect the security or strategic interests of India.
   iii. Affect the intellectual property rights or legitimate commercial interests of bidders.
   iv. Affect the legitimate commercial interests of the procuring entity in situations that may include when the procurement relates to a project in which the procuring entity is to make a competitive bid, or the intellectual property rights of the procuring entity.

b) The procuring entity shall treat all communications with bidders related to the procurement process in such manner as to avoid their disclosure to competing bidders or to any other person not authorised to have access to such information.

c) The procuring entity may impose on bidders and sub-contractors, if there are any for fulfilling the terms of the procurement contract, conditions aimed at protecting information, the disclosure of which violates (a) above.

d) In addition to the restrictions specified above, the procuring entity, while procuring a subject matter of such nature which requires the procuring entity to maintain confidentiality, may impose condition for protecting confidentiality of such information.

6. Scope of Work:

As part of the OSWAN project a State Wide Area Network Operations Centre (hereinafter referred to as “OSWAN-NOC”) shall be established for monitoring the OSWAN network infrastructure. The OSWAN-NOC shall analyse network problems, perform troubleshooting, communicate with various network maintenance officials / technicians and track problems through resolution. The key objective of the OSWAN-NOC is to ensure the health and availability of the components of the network laid under the OSWAN project. When necessary, OSWAN-NOC shall escalate problems to the appropriate stakeholders on the basis of an agreed escalation matrix.

The NOC Implementation Agency (NIA) to be selected through the RFP and shall be responsible for

- Implementation of the OSWAN-NOC.
- Operation & Maintenance of the OSWAN-NOC.

To monitor the OSWAN network the NIA would be responsible to build the Operation Centre area consisting of the Network Operation Area (OSWAN-NOC), server room, meeting room, etc.

The NIA shall be responsible for design, supply, installation and setting up of the necessary basic infrastructure for operation centre area in terms of civil, interior, electrical and Air-Conditioning System, Fire Prevention, Detection and Suppression System, Lighting system, Power to devices, multi-layer Physical Security, infrastructure like bio-metric based access-control system, CCTV/ surveillance systems, rodent repellent etc.

During the O&M phase the NIA shall be responsible for monitoring and maintaining the OSWAN-NOC so implemented. It is expected that the overall availability of the OSWAN-NOC shall be ~99.982% along with all its individual components.

The monitoring system to be implemented as a part of the OSWAN-NOC shall be capable of auto ticketing for any faults (prediction of faults) both for the components of the OSWAN-NOC and the network laid as part of the OSWAN project. Any fault or incident in the infrastructure of the OSWAN-NOC shall be repaired / restored by the NIA to meet the availability goal of 99.982%.

Any incident/ fault/ request related to the OSWAN network shall be auto assigned to the PIA team. The NIA shall configure the helpdesk to automatically route / assign ticket immediately as soon as an incident / alarm is triggered. The NIA shall be responsible to configure the NMS contact database in such a way that the information of the tickets are automatically sent via email to the relevant person or team.

6.1. Features of OSWAN-NOC

- **Network Supervision and Monitoring** - Monitor the complete network 24x7x365, to keep network and systems functioning in a stable operation mode. The NIA would be responsible to report any incidents in the service desk (automatically), assign same and follow-up with the resolution of the incident with the PIA. The NIA shall have an escalation mechanism in place and follow same

- **Configuration Management –** Assist the PIA team to ensure the proper configuration of network, systems and applications for the provision of reliable and high quality end-user services. The NIA shall assist the PIA with the discovery of the current configuration of the equipment and report to OCAC with the configuration report post the deployment / change in configuration.

- **Change Management** – Assist the PIA to ensure efficient day-to-day management of short-term network changes and optimization, including their implementation through a guided change management procedure based in ITIL v3 standards. The NIA shall be responsible for raising/ assisting in raising the change request in the Service Desk tool in consultation with the PIA and stakeholders. Following the change request procedure, closing the change request and reporting the change would be responsibility of the NIA.

- **Performance Management –** Provide insights from the reports of the EMS system to the PIA for efficient performance management procedures ensuring a reliable, high-quality network performance and service.

- **Service and Network Provisioning -** Define all necessary actions to be performed when a request for a new customer service is issued by customer care, and control the actions performed at OSWAN-NOC level or field level until completion. Monitor that the PIA ensures timely provisioning of the network / services as per the acceptable SLA.

- **Scheduled Activities Planning** – Document the regular plans for all scheduled activities, including preventive maintenance in the service desk and monitor the adherence. Respect a schedule, and achievement of the plan. This is linked to the change management function which ensures overall synchronization of all network activities.

- **IT and DB Management** – The NIA shall ensure day-to-day management of all the relevant application systems (Dashboard, NMS/EMS), IT systems (compute and network) and databases (administration, backups)

- **Security Management –** The NIA shall be responsible for defining and implementing the security policies, guidelines, and best practices, etc. for the OSWAN-NOC. The NIA shall also be responsible to check the status of the security

devices deployed for the backbone network and ensure that the PIA follows the ISO 27001 standards in maintaining same.

- **Quality Management –** Monitor the quality of services provided by the PIA based on the approved quality management policies, and ensure implementation and usage for competitive quality of service
- **Network Inventory Management** - Ensure consistent management of network equipment, and accurate, up-to-date documentation of it.
- **Spare Parts Management –** Assist the PIA in managing spare part handling and logistics to minimize repair/swap turn-around times for defective items. The NIA shall keep the status of the inventory of the spare in the system and report same regularly to OCAC.
- **Asset Inventory Management** - Ensure consistent inventory management for all assets including infrastructure, buildings, tools, spares, and equipment.
- **Escalation matrix management-** The OSWAN-NOC would ensure that a proper escalation database in place (emails, phone numbers) and should be capable of escalation of issues as per the escalation guidelines.

6.2. Design Considerations for OSWAN-NOC:

The envisaged OSWAN-NOC shall be equipped with modern infrastructure that will allow substantial economies of scale and designed with more energy efficiency. Consideration will be also given to the external environment. Some of the salient features of the OSWAN-NOC are listed as below:

Availability: Redundancy and high availability shall be provisioned for all the major components for OSWAN NOC using methods such as clustering, hot-standby, RAID and HSRP/VRRP etc. Non-IT components from LT Panel, PDUs, PAC, etc., will be in N+1 mode. UPS systems considered in N+N mode to cater full load of the critical components at the time of single electrical path failure. All IT components such as routers, switches, servers, etc., will be in high availability or cluster mode (active-active or active-passive).

The computing infrastructure shall be configured in High-Available mode such that redundancy is maintained. Equipment with dual redundant power supplies have been considered.

Automatic Transfer Switch ATS for single-power supply rack-mount equipment providing fail-safe redundancy has been considered. Virtualization may be used to improve the optimization of hardware used resulting in footprint of the hardware as well as power consumption. Virtualization shall also enable dynamic resource allocation in case of increase/decrease in load.

Flexibility: Flexibility is one of the major advantages of any Data Centre environment where different modules can be added based on the requirements. Here for the OSWAN-NOC for State Wide Area Network the modular approach will allow flexibility to add system resources based on requirements. The civil, electrical and mechanical infrastructure will be built at the initial stage with raw power arrangement as per requirement to bear the 100% load of the OSWAN-NOC for 5 years but UPS & the computing environment to be implemented based on requirements as on date. As the UPS is modular in nature it can be added with a modular approach. At initial stage, PACs will be as per current load and additional equipment will be added at a later stage to fulfil the requirements.

Scalability: The civil and passive components such as power panels, raised flooring for NOC room, PAC areas, BMS room, Intelligent BMS system, CCTV, access controls will be ready for the entire setup at the beginning of implementation of OSWAN-NOC. However, modular devices such as UPS, computing infrastructures, etc., will be scaled based on the demand to reduce the capital expenditure. With scalability as a prime feature of the OSWAN-NOC, the initial infrastructure requirement can be deployed without spending capital expenditure for future requirements. Another advantage of a modular based infrastructure is that the equipment can be implemented on demand and thus will reduce consumption of electricity and cooling.

As part of the overall design, scalability has been considered as an important consideration for all solution components to ensure that this OSWAN-NOC for the state of Odisha can support roll-out of any new other application/EMS/other modules or can support additional nodes of OSWAN without impacting the overall design. The scalability can support the applications for six to eight years considering the roadmap.

In the Compute Layer, modular and high performance computing systems have been considered since they provide horizontal scaling option with virtualization layer to host applications. The systems shall be configured with sufficient slots for future scalability.

The OSWAN-NOC network shall be configured with 10G links at the access layer and 40G links at the aggregate layer from day-1. The router shall be capable of supporting 10G ports and aggregation/core switch shall be capable of supporting 40G ports as well. All other network devices shall be configured with sufficient ports for future scalability.

The storage layer shall consist of unified storage for handling different type of data being stored. The storage shall be scalable for future requirements by adding more number of drives in the existing storage subsystem.

Security: The OSWAN-NOC shall be implemented with robust security controls across all layers which are required to ensure protection of critical information from any unauthorized access. All infrastructure hosting critical data and application shall be hosted in the Militarized Zone (MZ). In addition, consoles for managing network shall be in the Management Zone. The OSWAN-NOC will be protected from external and

internal threats by deploying Existing NGFW, Web Security with Proxy solution & AAA solution for controlling access to the S-NOC. The Existing NGFW have Intrusion Prevention System capability inbuilt for protection from advanced threats and have the capability to protect from DDoS attacks.

Performance: The infrastructure to be deployed at OSWAN-NOC shall be high-performance and state-of-the-art systems.

The Computing Infrastructure shall be Latest Generation x86_64 Bit processor. The Compute Infrastructure shall have high performance connectivity to network (10 Gbps) and storage (16 Gbps). The Network backbone for OSWAN-NOC shall be on 10G at the access layer and 40G at the aggregation layer on day-1 which can scalable up to 100G at the aggregation layer.

The proposed infrastructure shall be easily manageable from the serviceability perspective, thereby reducing the downtime of the critical applications. All the hardware infrastructure shall have redundant and hot swappable components such as fans, power supplies, disks, etc.

6.3. OSWAN-NOC Layout:

Following are the key design considerations for OSWAN-NOC.

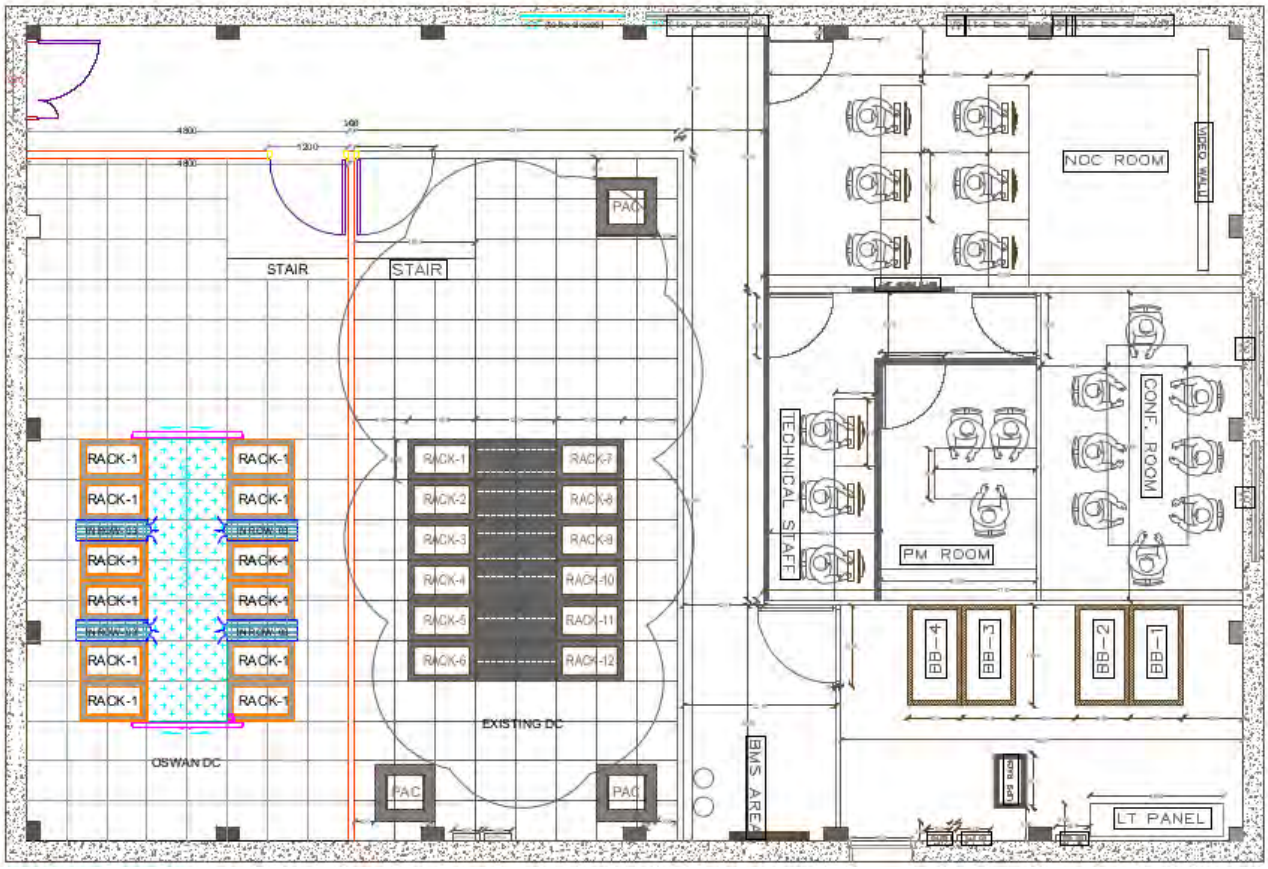
- Approx. 540 sq. ft. of total space has been allocated for OSWAN-NOC Server farm. Design of civil layout has been done considering the allocated area.
- Approx. 1200 sq. ft. of total space has been allocated for Help Desk. Design of civil layout has been done considering the allocated area.
- The bidder has to factor area for the BMS room and UPS Room, either in the area available for NOC or Help Desk.
- Approx. 300 sq. ft. of total space has been allocated for OSWAN Officials. Design of civil layout has been done considering the allocated area.
- Entire civil construction work and interior work will be done in the initial phase.

OSWAN-NOC Server farm will be allocated at Ground Floor, Help desk & OSWAN Official Area will be allocated at 1st Floor of OCAC Building. The physical layout of envisaged OSWAN-NOC is given below. Detail Layout will be chosen from best solution provided by the bidders and freeze during Implementation period. The bidder will make a survey of the site, at their own cost, before bid submission and the actual civil layout submitted by the bidder will be finalized in discussions with all the stakeholders.

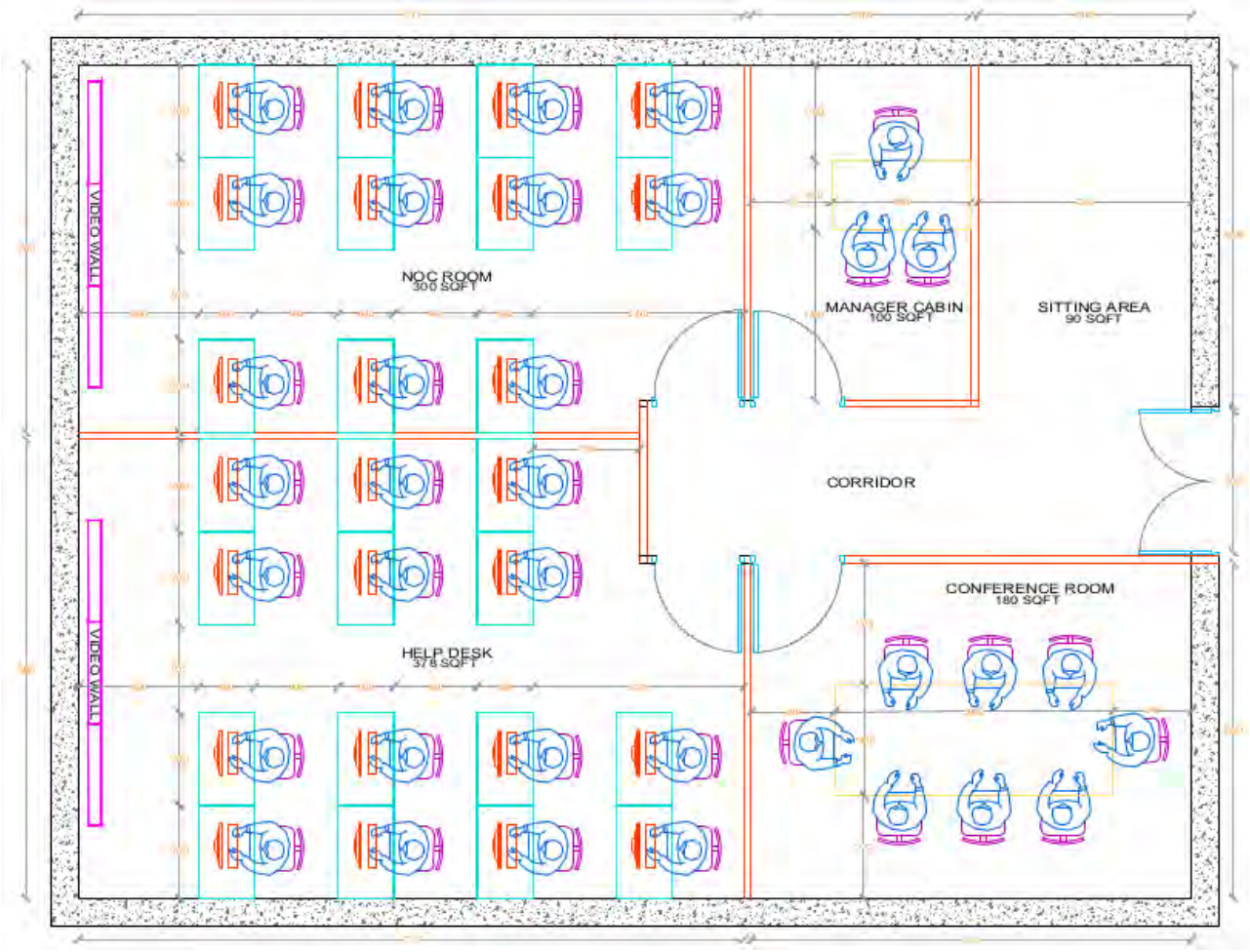
The scope shall comprise the design, supply, construction and testing of the proposed OSWAN-NOC including all enabling works. All Works shall be carried out as per the proposed design and specifications and in accordance with the requirements of all relevant Indian standard codes.

Bidder is advised to visit the existing facility and conduct a detailed survey to understand the existing facility. Existing facility houses BHARATNET data centre along with supporting areas. BharatNet DC was designed and built considering IBMS and Electrical components scalable for OSWAN NOC.

Bidder is advised to quantify the existing systems and design a solution suitable to be integrated with the existing systems. Electrical panel is available on site which also feeds BharatNet DC and supporting areas. Supply for PACs, UPS and other load must be fed from existing LT Panel. Bidder is supposed to design safety security components in a manner so as only field devices needs to be procured and existing equipment like Fire alarm panel should be used.



OSWAN NOC Room



OSWAN Helpdesk Room

Bidder to propose their solution by assessing the project requirement and should supply adequate Non-IT & IT-Infrastructure (Server, Storage to implement NMS and other management solution).

6.4. Design Consideration of Non-IT Infrastructure:

OSWAN-NOC shall be built with Server Area, NOC Help Desk Sitting Area, UPS and Battery Room, Meeting Room, Manager Room etc. Indicative sizes of the above stated functional areas are given in the table below. The sizing in the table is a reference to provide an overall idea of the required space in OSWAN-NOC. The size may vary due to dimensions of the final list of components (e.g. rack cabinet size) proposed for the OSWAN-NOC. At the time of interior design (civil) and construction face, best standards for building NOC shall be followed by System Integrator for the following work:

- **Civil & Interior Works** (Including Dismantling & Construction of Brick work, masonry work, painting, Partition, False floor, Raised Floor, False ceiling, Water proofing, etc.
- **Electrical System Work** (Including electrical panel, Earthing, NOC internal electrical wiring, DB, Switchgears, Lighting & fixtures, etc for all NOC Areas, DC Areas, Helpdesk Areas & Office Areas)
- **Modular UPS** with VRLA battery for minimum 30 Min Backup on full load for the Server Farm Area and Helpdesk areas.
- **Precision Air Conditioning System** (In Row Cooling for the Server Farm Area)
- **Comfort Air Conditioning** for the Helpdesk Areas & Office Area
- **Fire Suppression and Detection System**
- **VESDA System**
- **Water Leak Detection System**
- **Access Control System**
- **IP CCTV System**
- **Public Address System**
- **Rodent Repellent System**
- **Fire extinguisher Solution**
- **Building Management Solution**
- **Video Wall (3x2) Solution**
- **Passive Networking Solution**

6.5. Design Consideration of IT Infrastructure:

While designing the solution of IT infrastructure, we have assessed the current and future demand of Odisha SWAN Project. We have considered major components such as servers, storage, backup solution, networking components, logical security components, NMS/EMS solution, Virtualization and software licenses as a part of the solution.

OSWAN-NOC is envisioned to monitor the entire Odisha State Wide Area Network (OSWAN) project. Initially this will cater the requirement to monitor existing equipment under Vertical OSWAN & Horizontal OSWAN whereas later part of the project, the OSWAN-NOC will be utilized to monitor the Equipment to be installed under OSWAN 2.0 Project.

6.5.1. Network Management Solution (NMS):

The solution shall able to support the proposed hardware and software components deployed by the PIA over the tenure of the contract. The solution shall be capable of providing early warning signals to the Helpdesk Agents on the performance issues, and future infrastructure capacity augmentation. The solution shall also support single pane / dashboard with visibility across multiple areas of Network for monitoring. NIA is required to design, supply, install, customize, test, implement, rollout and maintain the NMS application and hardware as per the requirements.

The proposed solution comprising of following components.

- **Network Discovery & Monitoring:** The NMS solution shall be able to do a complete discovery of IT environment across distributed (i.e., physical, virtual, network, application) and heterogeneous environment and provide a clear and visual mapping of IT infrastructure to business services.
- **Network Fault Management:** This system shall provide fault, performance and configuration management for multivendor IP Network.
- **Network Performance Management:** The solution shall provide real time visibility into top conversations happening in the network and support extensive reporting capability with 1-minute granularity, custom 0 breakdowns (for analysing flow data by user-selected combination of data types, such as source and destination IP, address ranges, port, protocol, QoS classes etc.), adjustable data retention settings, flexible grouping controls, and the ability to store years of rolled-up data.
- **Reporting and Dashboards:** The Network Management System shall have the ability to provide SLA reports on the following metrics:
  - Availability
  - BW utilization
  - Resource utilization (in WAN / LAN)
  - Response Time
  - Throughput
  - Latency
  - Jitter
  - Loss ratio
  - Downtime for both link and device
  - Failure Frequency

- Mean time to repair
- Mean time between failures
- Uptime
- Error statistics

➢ **Automation:** Solution shall be having ability to forecast the schedule for a future date and simulate the flow of jobs in terms to the estimated start and end times of jobs and business services with option to add what-if scenarios for better simulation. Solution shall be able to execute BW Programs, Data Archiving Programs & Business Objects reports and provides out of box interface for it. Solution shall have ability to integrate with any enterprise database to schedule and run the SQL scripts, open queries, Stored procedures and SQL Server Integration Services (SSIS) packages and provides out-of-box interface for it. Not through wrapper scripts.

6.5.2. Syslog server implementation

The bidder has to implement syslog server for OSWAN on open source platform. The syslog server must fetch logs from all network devices under OSWAN.

6.6. Detailed Scope of Work:

OCAC proposes to setup Odisha State Wide Area Network Operation Centre for monitoring WAN Links and Service desk / HELP DESK Tool for ticketing system. In order to check and verify the Service Level Expectations/ Agreement (SLA), to analyse network traffic, bandwidth utilization, configuration of alerts and reports, there is need for setup of Network Operation Centre. This will also help in representation of the SHQ, DHQ, BHQ & HO network, links, network equipment, infrastructure management and provide a real-time, at-a-glance portrayal of the entire OSWAN Network.

The Scope of work necessarily, but not exclusively includes the following activities:-

The proposed Enterprise Network Management Solution will able to provide a unified platform for providing end to end monitoring of IT Environment and cohesive integrated drill down view to report, analyse, isolate the root` cause with inherent and inbuilt ability to integrate with other performance and response analysis tool. The Enterprise Network Management Solution provides:

- Single platform to monitor and report on the Infrastructure components/services
- Dynamic network topology, Network Discovery and Reporting
- Fault Analysis & Mobile Integration
- Integrated Configuration Management for Network Devices
- Advanced IP Services Management
- Managing Network Service Levels
- Deployment Features & bulk firmware upload

- Integrations with other performance tools
- Protocol-Based Traffic Analysis, net-flow and response time analysis.
- Performance & Availability of heterogeneous networking devices
- Infrastructure Monitoring Requirement
- Inventory Management such as asset report, organized by vendor name and device, listing all ports for all devices.
- Trouble-shooting & RCA
- On Demand Dashboard for daily & historic network health, reports.
- Change Management, Incident Management and knowledge management.
- Capacity Management, Backup Management.
- Multivendor Support and extendibility
- Service Desk Management & Ticketing

6.6.1. Site Survey

- Interested bidder may visit the site @ OCAC, to survey the proposed OSWAN-NOC control room site, during the working days for actual assessment of project site, before the submission of the bids.
- The survey shall include the details of existing Odisha Wide Area Network Topology, protocol, Existing Devices the location positioning and establishment of the NOC.
- The bidder may contact Sh. Arun Bairiganjan, SA, OCAC (+91-9937312169)/Sh. Rajib Kumar Dash, Consultant, OSWAN (+91-9438670199) before visiting the site.
- The cost of survey would be borne by the bidder. OCAC holds no responsibility on the cost undertaken by the bidder for site survey.

6.6.2. Implementation phase

- **Site Preparation**: Site preparation structure for OSWAN-NOC would include false ceiling, lighting, glass and gypsum / plywood partition, flooring, access control, fire safety and command centre furniture.
  External civil construction may or may not be a part of the scope of the bidder, discretion of developments and future decisions of OCAC. The scope may be revised at a later stage with timely intimation to the bidder. Civil construction inside the identified OSWAN-NOC space / area would be under the scope of the bidder.
- **Site Clearance:** The successful bidder in coordination with OCAC shall arrange for necessary clearances including statutory and regulatory which shall enable them to undertake civil, electrical, and mechanical works including building modification, partitioning, installation of electrical component, cable laying etc. at the OSWAN-NOC site.

6.6.3. Setup of Modular Data Centre and NOC at SHQ

OCAC intends **to Setup a Portable/modular Server Firm enclosure with prefabricated components and operate, manage the same for a period of 5 years.** The Portable/modular Server Firm enclosure will have to be set up in an area of approximately 15' X 25' to accommodate at least 06 42U racks for server, storage and other IT components and 06 Network racks to accommodate Network equipment of OSWAN.

Also OCAC intends to set up the Network Operation Centre (NOC) in an area of approximately 40' X 30' in another room at OCAC Centre to provide operational and management services through MSP with greater reliability, availability and serviceability. The minimum specified scope of work to establish a Server Farm and Network Operation Centre is mentioned below.

1. Setting up **Portable** Server Farm enclosure with all non-IT component installation those are required for Data Centre e.g BMS, Surveillance, HVAC, Fire control system, precision air conditioning, UPS System etc.. if required, The physical room for Portable Server Firm enclosure needs to be closed with brickwork, the flooring should be done to bear the load of the Portable Server Firm enclosure with fully populated IT components. The work should be completed within 8 weeks time.
2. Setting up the Network Operation Centre with an arrangement to accommodate 25 resources. The work also includes civil work, Split Air Conditioner, Tables, chairs, cup boards, Conference Area, PM room, Video Wall installation, etc. The timeline for completion is 8 weeks.
3. The Block Diagram for OSWAN NOC is mentioned at ***Clause 6.3***.

The bidder has to prepare a design diagram of the room where the Portable Server Farm enclosure will be installed and submit the same along with the bid. The design should be optimal and economical and accommodate as many as server racks in the portable enclosure. However minimum 6 numbers of server racks (42 U) and 6 numbers of network racks need to be accommodated within the enclosure besides other components required for Data Centre such as Precision A/C, UPS System, Fire Management System, Humidity control system, Access Control system etc.. The major components like UPS, Precision AC and Rack PDU should be from a single OEM for better management and maintenance. The clean area available for installation of Portable Server Farm enclosure is 25' (L) X 15' (B) X 9' (H). The Portable Server Farm enclosure should have the features of a Tier – II Data centre. The layout and design to be submitted by the bidder, should include minimum following designs and layouts

- Basic Layout of the room and Portable Server Farm enclosure
- UPS System details

- Access Control System Layout for the room and Portable Server Farm enclosure
- False ceiling Layout of the room
- Electrical layout of the room and Portable Server Farm enclosure
- Lighting Layout of the room and Portable Server Farm enclosure
- Loose furniture details with fixing layout (if required)
- Fixed furniture details (if required)
- Civil addition and alteration details with layout
- Internal/ sectional elevation (if required)
- Cabling Layout for the room and Portable Server Farm enclosure
- CCTV Layout for the room and Portable Server Farm enclosure
- Rodent Repellent Layout for the room and Portable Server Farm enclosure
- Fire Extinguisher Layout for the room and Portable Server Farm enclosure
- Water Leak Detection System layout for the room and Portable Server Farm enclosure
- Other drawings as required by the OCAC from time to time.

Civil work

The room for Portable Server Farm enclosure has to be sealed in such a way that external air should not enter into the area. For this necessary civil work may be required to be done. The details of the civil work required to be carried out need to be assessed by the firm and concrete proposal thereof to be given in the bid.

Interior work

The interior of the room of Portable Server Farm enclosure should be as per Data Centre standards. The wall should be painted with eye soothing colour. The false sealing should be made below the roof of the room with proper provisioning of light and air conditioning etc.. Necessary partitioning if required has to be done. The entrance side of the Server Farm should be transparent above 2’6” from the ground. The bidder is free to give the best design as per new technology and standards. Site strengthening work (if any) would be the responsibility of bidder and it would ensure floor loading capacity (superimposed live load) of minimum 500 kg / sq.ft.

Electrical work and lighting

The bidder has to do all the electrical wiring inside the room and Portable Server Farm enclosure using certified best materials available to ensure that no short circuit happens at any point of time. The bidder has to provide wiring from each rack to the power distribution points of UPS of 40KVA with N+N architecture and with provision for future expansion up to 40KVA with N+1 architecture. The complete wiring for Air Conditioning has to be done by the bidder starting from the power

source. Proper insulation should be made so that electrical signal should not interfere with others. The electrical wiring should be such that additional power point should be made available for each rack keeping in view the average load factor in the rack as 6KVA for Server Rack and 4KVA for Network Rack.

The electrical cabling Work shall include the following:

- Main electrical panel in OCAC
- Power cabling
- UPS point wiring
- Power Cabling for Utility component and Utility Points etc
- Online UPS
- Separate Earth Pits for the component (Server Firm, UPS, PAC, etc.)

  The distribution of power from the UPS room to the following shall be considered:
- All proposed component for the production environment
- Existing servers and other component
- Final Distribution shall be through Power Distributions Units (PDU)/MCB Distribution Boxes. Power in the racks and other component's shall be provided with two sockets with power coming from separate UPS in each of these sockets.
- The bidder is required to maintain electrical distribution paths for the cabling inside the server farm area in OCAC

Specifications for Electrical Cabling – Fire retardant cables of rated capacity exceeding the power requirement of fully blown configuration of the existing and proposed component to be used. For expansion needs suitable redundant power points to be provided at suitable locations. All materials used shall conform to IS standards as per industry practice.

- Bunching of Wires – Wires carrying current shall be so bunched in the conduit that the outgoing and return wires are drawn into the same conduit. Wires originating from two different phases shall not be run in the same conduit.
- Drawing of Conductors – The drawing Aluminium / Copper conductor wires shall be executed with due regards to the following precautions while drawing insulated wires in to conduits. Care shall be taken to avoid scratches and kinks, which cause breakages.
- Joints – All joints shall be made at main switches, distribution boards, socket outlets, lighting outlets and switch boxes only. No joints shall be made inside

conduits and junctions boxes. Conductors shall be continuous from outlet to outlet.

- Mains & Sub-Mains – Mains & sub-mains wires where called for shall be of the rated capacity and approved make. Every main and sub-main shall be drawn into an independent adequate size conduit. Adequate size draw boxes shall be provided at convenient locations to facilitate easy drawing of the mains and sub-mains. An independent earth wire of proper rating shall be provided. The earth wires shall run along the entire length of the mains and sub-mains.
- Load Balancing – Balancing of circuits in three-phase installation shall be planned before the commencement of wiring.
- Color Code of the Conductors – Color code shall be maintained for the entire wiring installation, Red, Yellow, Blue for three phases and “OFF” circuit black for neutral and green for earth (or bare earth).
- Fixing of the Conduits – Conduits junction boxes shall be kept in position and proper holdfasts shall be provided. Conduits shall be so arranged as to facilitate easy drawing of the wires through them. Adequate junction boxes of approved shape & size shall be provided. All conduits shall be installed so as to avoid stream and hot water pipes. After conduits, junction boxes, outlet boxes & switch boxes are installed in position their outlets shall be properly plugged so that water, mortar, insects or any other foreign matter does not enter into conduit system. Conduits shall be laid in a neat and organize manner as directed and approved by OCAC or person on their behalf. Conductors shall be planned so as not to conflict with any other service pipe lines / ducts.
- Protection – To minimize condensation or sweating inside the conductors all outlets of conduit system shall be adequately ventilated and approved by the proper competent authority. All screwed and socketed connections shall be adequately made fully water tight by use of proper jointing materials.
- Switch-Outlet Boxes and Junction Boxes – All boxes shall conform to all prevailing Indian Standards. The cover plates shall be of best quality Hylam sheets or ISI grade Urea Formaldehyde Thermosetting insulating material, which should be mechanically strong and fire retardant. Proper support shall be provided to the outer boxes to fix the cover plates of switches as required. Separate screwed earth terminals shall be provided inside the box for earthling purpose.
- Inspection Boxes – Rust proof inspection boxes of required size having smooth external and internal Finish shall be provided to permit periodical inspection and to facilitate removal and replacement of wires when required.

The room and Portable Server Farm enclosure should be lighted properly so that each and every point inside the firm made visible.

UPS System

Uninterruptible Power Supply System with Sealed maintenance Free VRLA Battery for 30 minutes back up to work in N+N redundant configuration to be installed to maintain the power availability for the Racks.

Air Conditioning

Since Server Farm zone is a critical area, air conditioning system (Row based precision air conditioning) should be exclusively installed to maintain the required temperature within the room and Portable Server Farm enclosure. Operation Centre zone can have a common air conditioning system for comfort. The general requirements for the Server Farm are as specified below:

The Portable Server Farm enclosure should be provided with Row based precision air conditioning on a 24 x 7 x 365 days operation basis. The Air-conditioning system should have either on N+N or N+1 redundancy. The units should be able to switch the air conditioner on and off automatically and alternately for effective usage in pre-defined sequence. Precision Air Conditioning systems specifically designed for stringent environmental control with automatic monitoring and control of cooling, heating, humidification, dehumidification and air filtration function should be installed. The air is to be distributed evenly

Temperature and humidity

The Portable Server Farm enclosure should be controlled with precision environment parameters. The temperature inside Server Farm area should be maintained at 22 degree centigrade with a precision of ± 2 degrees and humidity 50% +/- 5RH. The Precision Air Conditioning shall be provided for the Portable Server Farm enclosure with 99.5% up time. Best technology that would minimize the air-conditioning load and ensure precession air conditioning may be suggested by the bidder.

Installation of Fire Detection and Control System

The selected bidder has to install proper fire management (Detection and Suppression) system for detection and control of fire inside the Portable Server Farm enclosure. The system should be able to automatically operate in case of incident of fire/smoke.

Installation of CCTV Surveillance systems

The Selected bidder will have to install a CCTV surveillance system inside the room and Portable Server Farm enclosure so that each and every activity within the Portable Server Farm enclosure and room would be captured and stored in a DVR/NVR. The Server Farm Operation centre shall monitor the activities within the server room on real time basis. Necessary cabling and installation of DVR/NVR, Display unit will be the responsibility of the bidder.

Installation of Access Control System

As Server Farm area is a highly secured zone, unauthorised access to the Server Farm needs to be avoided. Hence access to the server Farm area has to be given to authorised officers only. Therefore an Access Control System has to be installed for Server Farm with feature for biometric, card, eyries based access.

Rodent repellent

The entry of Rodents and other unwanted pests shall be controlled using nonchemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the flooring and ceiling to repel the pests without killing them.

- Configuration: Master console with necessary transducer
- Operating Frequency: Above 20 KHz (Variable)
- Sound Output: 50 dB to 110 dB (at 1 meter)
- Power output : 800 mW per transducer
- Power consumption : 15 W approximately
- Power Supply : 230 V AC 50 Hz
- Mounting : Wall / Table Mounting

Acceptance Testing and Commissioning

OCAC shall review and would also conduct audit of the process, plan and results of the Acceptance Test carried out by the successful bidder. OCAC would issue certification of completion for which OCAC shall verify availability of all the defined services as per the contract signed between the successful bidder and OCAC. The successful bidder shall be required to demonstrate all the services / features / functionalities as mentioned in the agreement.

Commissioning shall involve the completion of theOCAC site preparation, supply and installation of the required components and making the Server Farm at OCAC Centre available to OCAC for carrying out live Operations and getting the acceptance of the same from OCAC. Testing and Commissioning shall be carried out before the commencement of Operations.

The final acceptance shall cover 100% of Server Farm after successful testing by OCAC or its third party monitoring agency; a Final Acceptance Test Certificate (FAT) shall be issued by OCAC. The date on which Final FAT certificate is issued shall be deemed to be the date of successful commissioning MDC at OCAC.

Prerequisite for Carrying out FAT activity:

- All documentation related to Server Farm and relevant acceptance test document (including IT Components, Non IT Components etc.) should be completed & submitted before the final acceptance test to OCAC.

Network Operation Centre

This will have provision for monitoring the OSWAN activities round the clock and sitting arrangement for minimum 25 resource persons. This will also be a secure area where access control system need to be installed. This area shall be air conditioned using suitable capacity split Air Conditioner. The total design of the NOC has to be provided by the bidders along with bid. Necessary furniture and fixtures shall be provided by the selected bidder. The broad activities are

- Design layout of the NOC
- Air Conditioning
- False ceiling
- Flooring (if Required)
- Electrical and networking wiring
- Lighting
- Fire detection and control system installation
- BMS control unit set up
- Video wall Setup
- Access control system installation
- Furniture and fixtures set up
- Development of cup boards

6.6.4. Other scope

Change Management

Plan for changes to be made - draw up a task list, decide on responsibilities, coordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage documentation.

Vendor Management

- Coordination with all the project stakeholders to ensure that all Server Farm and NOC activities are carried out in a timely manner.
- Coordination with vendors and OEMs to ensure that time and equipment dependencies are optimally managed
- Selected bidder shall coordinate and follow-up with all the relevant vendors to ensure that problems and issues are resolved in accordance with the SLAs agreed upon with them.
- Selected bidder shall also ensure that unresolved issues are escalated to concerned person in accordance with the escalation matrix.
- Selected bidder shall maintain a track of SLA performance for vendors.
- Selected bidder shall maintain database of the relevant vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.
- Selected bidder shall draw a consolidated quarterly SLA performance report across vendors for consideration of OCAC.

- *Physical Infrastructure Management and Maintenance Services*

  All the devices that will be installed in the OCAC as part of the physical infrastructure should be manageable with BMS and shall be centrally and remotely monitored and managed on a 24x7x365 basis. Industry leading infrastructure management solution should be deployed to facilitate monitoring and management of the MDC.on one integrated console. The physical infrastructure management and maintenance services shall include
  - Proactive and reactive maintenance, repair and replacement of defective components (Non-IT). The cost for repair and shall be borne by the selected bidder.
  - The selected bidder shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met. To provide this service it is important for the selected bidder to have back to back arrangement with the OEMs.

- The selected bidder needs to provide a copy of the service level agreement signed with the respective OEMs.
- Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected bidder fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.
- The selected bidder shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by OCAC at any time.

- The selected bidder shall procure and supply all Non IT components. The selected bidder would be required to undertake all the necessary civil & interiors, electrical, plumbing and mechanical works including false ceiling/flooring, partitioning, installation of electrical component, cable laying etc and other infrastructure or services to create the Non- IT/ Physical Infrastructure.

- Installation shall mean to install and configure / integrate every component and subsystem component, required for functioning of the Server Farm.

- Based on generic solution design, minimum capacities and specifications for the components have been worked out and detailed in **Annexure-1**. However, these are only bare minimum requirements and the bidder is at liberty to suggest better solutions to meet the overall SLA requirements.
- Power cabling inside Server Farm and Control area shall be of copper. The cables and conduits used inside the zones shall be of FRLS quality. Signal referencing copper Earthing using braided copper wire of 6 Gauge.

- Currently OCAC has 3X400 KVA DG Set of Make Kiloskar, Model – WS400KG and the same shall be used for OSWAN. OCAC may procure DG set on need basis considering the power load populated

- The Selected bidder shall provide monitoring and management services for an agreed service window during the agreed contractual period from the date of final acceptance test. The scope of the services for overall Physical infrastructure management during this period shall include Monitoring, Administration and Management of the Non-IT infrastructure.

- BMS for OSWAN NOC & Helpdesk room, shall be integrated with DG Set and UPS.

- BMS for NOC Room, Helpdesk room & UPS Room, can be provisioned with the existing BMS of Bharanet as an extension or the bidder may go with new BMS solution for these room. The bidders has to submit the BoQ accordingly. In case of

new BMS solution, the bidder may visit the site to identify the place for setup of separate BMS room.

Acceptance Testing and Commissioning

Likewise Modula DC Acceptance Testing and Commissioning will be done for NOC also. Prerequisite for Carrying out FAT activity:

- Successful shifting of Server, Racks, Network Devices, and other accessories. Documentation related to all shifting, Asset tagging, etc. should be completed & submitted before the final acceptance test to OCAC.

Important : No products supplied under the RFP should be end of life or end of support. No equipment model should have been introduced in the market not later than 1 years back as on date of the submission of bid.

- ***Implementation of IT & Non-IT Infrastructure:*** The successful bidder should carry out:
  - Complete supply, installation and commissioning of required IT, Non IT and civil infrastructure at all the designated locations of the OSWAN-NOC as identified.
  - The bidder is responsible for calculation of Hardware sizing like no. of server to run the NMS & Ticket Management software successfully for a period of 5 years from date of successful installation.
  - Required storage space to be provided by OCAC/OSDC for this project, or the bidder may go with new storage solution beyond storage @ OSDC. In that scenario bidder has to provision & ensure all type of onsite support for the new storage solution provided.
  - In case, the bidder will go with existing storage solution at OSDC, provisioning of the connectivity between OSWAN NOC at ground floor and OSDC at 2nd floor for SAN connectivity, has to be ensure by the bidder.
  - Successful bidder shall submit stage-wise reports and it should be done strictly in accordance with the scope of work in the document.
  - Successful bidder is expected to adhere to all technical and non-functional specification for IT, Non-IT and civil infrastructure.
  - Any additional design guidelines as provided in the tender document / proposed solution document has to be achieved as per established delivery time lines.
  - The Bidder shall study and understand the existing setup at SHQ and shall develop a project implementation plan indicating milestones and deliverables to OCAC. The bidder shall ensure that integration should be seamless and within stipulated timelines.
  - A detailed project plan for the implementation of OSWAN-NOC is to be provided during the Kick-off meeting by the successful bidder.

- A work break down structure with all milestones for the entire commissioning time line is to be provided by the successful Bidder.
- The successful bidder would be required to submit detailed design documents with all necessary design drawings for all IT, Non IT and civil infrastructures and would be approved by OCAC Technical Committee before actual execution of work.
- A supply schedule for all materials with make and model is to be prepared and submitted in line with the work break down structure of the project plan.
- All materials are to be dispatched as per expected delivery time lines with no additional dispatch or delivery costs.
- Any deviation from the expected time lines of delivery is to be intimated in advance for appropriate actions and reason.
- The materials should be brand new and as per the tender specifications/requirements
- Bidder should take care of Insurance against the material loss.
- The bidder shall supply skilled manpower for OSWAN Network Operations Centre (OSWAN-NOC) operations over a period of 5 years at OCAC location as detailed in this document.
- Bidder has to coordinate with the existing manpower of OSWAN FMS at OCAC for Operation of OSWAN NOC.
- Implementation Agency shall ensure 99.98% uptime & availability of all NOC devices and tools.
- The deployed solution should be scalable for 3000 nodes and 40 Help desk engineers.
- Bidder is expected to offer solution covering all the functionality as mentioned in RFP. Incomplete responses are liable for dis-qualification.

6.6.5. Cloud Virtualisation

Supply, Installation, Configuration, upgardation of solution to latest running version & Comprehensive Warranty Support of the supplied cloud virtualization. The provided solution should act as a single umbrella for management and operational.

6.6.5.1. Virtualization Functionality Requirement

a. Detaild design and implementation document should be provided before installation.
b. Installation of server hypervisor, SDN & cloud management platform on 5 no of hosts.
c. Workload segregation.
d. Testing of Deployed solution.
e. Knowledge Transfer specific to Virtualization Deployment

f. 24 x7 support for 5 Years required from OEM as and when required for resolving all OS (Operating Systems) & Virtualisation solution related issues, including re-installation of OS or re-clustering or re-configuration and other required software procured in this RFP, during support period without any extra cost to the OCAC.
g. Bidder should upgrade the Virtualisation solution supplied under this RFP and other related software whenever there is new version released for such upgrade without any cost to the OCAC during the contract period including ATS etc.
h. Bidder should provide virtualization solution & its related other software licenses with comprehensive support of 5 year without any extra cost.
i. Bidder has to carryout hardening of OS (Operating System), patch management activity and other configuration on OS, Virtualisation and its related software, etc., (which is provided under this RFP) as per the requirement of OSWAN.
j. Technical and functional documentation of the entire project should be submitted to OCAC in Printed Book Format.
k. The bidder shall provide perpetual licenses for all software components proposed in the solution and should be in name of OCAC.
l. The bidder shall propose Support & Subscription services from the OEM with unlimited number of support requests, remote support, access to product updates/upgrades and 24x7 supports.
m. The bidder shall propose Plan & Design/ Architecture services from the OEM. The OEM shall conduct a health-check of the deployed solution and submit a report indicating compliance to reference architecture and best practices. The entire software supplied under this RFP must be installed and configured by OEM only. The bidder to make necessary arrangement for the same and OCAC will not pay any additional cost for implementation by OEM.
n. Detailed process documentation, SOP's and management of solution should be created and submitted before project signoff.
o. Design, deployment, implementation and validation has to be done by OEM professional services team.

6.6.5.2. Training

The Bidder will be responsible for training the OCAC/OSDC/OSWAN Team in the areas of parameterization, implementation, migration, operations, management, error handling, system administration, upgrade etc. The training should at least cover the following areas and detailed each and every module installed as required for the solution to work efficiently and smoothly:

i. Functionality available in the solution
ii. New functionality customized (if any)
iii. Parameterization
iv. Impact Analysis
v. Generating various MIS/EIS reports from the solution provided

vi. System and Application administration
vii. Log analysis and monitoring

All the trainings would be held at the OCAC sites and the Bidder has to organize the trainer from OEM.

6.6.6. Shifting of Existing IT Infrastructure to proposed NOC:

- The existing OSWAN Infrastructure at Bharat-Net NOC comprising of Racks, servers, switches, Gateways, Network elements, VC MCUs, Sensitive IT Equipment, Other IT hardware and associated software in the OCAC Building is to be shifted to the new OSWAN NOC on as is where is basis with a downtime of maximum of 48 hours. Shifting of the equipment involves un-mounting, packaging(if required), shifting, from the existing Bharat-Net NOC room and un-packaging, mounting of the equipment at new OSWAN NOC.
- Physical installation of network equipment and physical connectivity to all links with network switches have to be done.
- Integration of active equipment (Network, Security, Servers, VOIP and VC system) using UTP and OFC cable have to be done.
- The selected bidder will be responsible for taking adequate insurance cover for shifting the existing equipment.
- Any other work related to shifting not included in the above points need to be taken care by the selected bidder at no additional cost to OCAC.
- The selected bidder has to coordinate with all the ISPs for shifting of ISP link.
- Bidder should analyse and study the existing infrastructure located at SHQ, and provide the solution for migration.
- Bidder accordingly shall implement the solution.
- Connectivity between OSWAN Firewall and SECLAN Firewall.

6.6.7. Operation and Maintenance:

The scope of work for the bidder is limited to equipment / component procured as part of OSWAN-NOC. Later if any additional hardware or software is required in NOC, all additional hardware and software required would be procured by OCAC and would be maintained by the bidder. However, for monitoring these managed device if any additional hardware / software / licenses are required then the cost will be borne by OCAC.

- On-site comprehensive maintenance and provisioning of services of all the ICT Infrastructure and their components supplied with a provision of onsite spares on 24x7x365 basis after successful execution and acceptance by OCAC.
- Onsite support for NOC Operations on 24x7x365 basis by qualified and trained personnel for a period of 5 years to ensure high service availability.
- The successful bidder should provide 24 x 7 x 365 operating and maintaining services for a period of 5 years from the date of Go Live for OSWAN-NOC.
- The successful bidder is required to provide the comprehensive onsite maintenance with part replacement for all the IT and Non IT equipment.

- The successful bidder shall be responsible to ensure adequate and timely availability of spare parts needed for repairing the equipment/ parts.
- To provide this service the selected bidder must have back to back arrangement with the respective OEMs/ OEMs authorized partner.
- The successful bidder has to make necessary arrangements of spares for catering maintenance needs of equipment/parts during entire engagement period at no extra cost to the client.
- Root Cause Analysis of the incidents (Major & Minor) to identify threat sources and proactive measures to prevent recurrence.
- Successful bidder will be responsible to store logs in industry standard solution and format for extraction and sharing with other solutions/ agencies.
- The successful bidder shall also provide a detailed process for managing Incident Response (IR) describing each phases of the process – prepare, identify, contain, eradicate, recover and learn from the incidents responded to.
- Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact.
- The services and solutions in scope should be designed with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime and availability.
- Preparation of OSWAN-NOC SOPs and User manuals, BCP plan, Exit Management Plan, Helpdesk management, Change Management, etc. Documents.

6.6.8. Partial Acceptance Test (PAT)

After completion of mentioned stages of work as per timelines provided in the RFP, the successful bidder shall request for Partial Acceptance Test (PAT).

Partial Acceptance Test will be conducted by the Consultant / PMU in accordance with the timelines, scope of work as mentioned in the RFP and the solution documents proposed by the successful bidder and accepted by OCAC. The Consultant / PMU will prepare and submit the report of PAT to OCAC and subject to its acceptance, it shall be deemed as completion of Partial Acceptance Test (PAT).

6.6.9. Final Acceptance Testing (FAT) and Go-Live:

FAT reports will be verified and approved jointly by OCAC, Consultant and successful bidder following which the commissioning certificate will be issued by OCAC. All Civil, IT and Non IT systems are to be installed and tested as per the tender and continuous status reports are to be submitted. Commissioning certificate will be issued by OCAC after completion of the project components as per scope of work.

The test shall include the following:

- All civil, electrical, air conditioning works, etc., are completed as per the RFP specifications and solution documents proposed by the successful bidder and accepted by OCAC.
- All hardware and software items must be installed at OSWAN-NOC site as per RFP specifications and solution documents.
- Availability of all the defined services shall be verified. The successful bidder shall be required to demonstrate all the features/facilities/functionalities as mentioned in the RFP and solution documents.
- The PMU in consultation with OCAC shall define detailed test plan.
- The successful bidder will arrange the test equipment required for performance verification and also provide documented test results.
- The successful bidder shall be responsible for the security compliance of the infrastructure and network before the final acceptance test.
- The successful integration of all assets and its functioning in the prescribed manner.
- All points of Partial Acceptance Test (PAT) if any, should be addressed and resolved before the final acceptance test.

7. Manpower for OSWAN-NOC:

Sr. No	Manpower Designation	No. of resource	Shift details
1.	NMS Specialist	01	• Resource available during the time specified. • All days of week with shift rotation with the existing NMS Specialist, except Sunday / State Government holidays. • Time: 10:00 am to 06:00 pm and whenever required during emergency downtime.
2.	BMS Specialist	01	• Resource available during the time specified. • All days of except Sunday / State Government holidays. • Time: 10:00 am to 06:00 pm and whenever required during emergency downtime.
3.	Electrical	03	• Resource available during the time specified. • All days of except Sunday / State Government holidays. • Time: 10:00 am to 06:00 pm and whenever required during emergency downtime.
TOTAL		**05**	

Note:

(1) The above table is indicative only. The bidder can propose a shift arrangement as per his own convenience and optimal utilization of resources.

(2) *In any case of emergency or urgent leave, an equivalent replacement should be present with prior approval from department SPOC / Nodal officer.*

(3) *During any critical incident, manpower should be available even beyond the specified working hours.*

(4) *The Manpower to be deployed on-site should be under the payroll of the bidder.. However, bidder needs to have similar resources as given in the RFP on their payroll. Interview would be conducted for the payroll resources.*

(5) *Bidder has to coordinate with the existing OSWAN FMS Team for the operation of the NOC*

7.1. Qualification:

Sr. No	Manpower Designation	Desirable Qualification and Experience	Roles & Responsibilities
1.	NMS Specialist	• B.E/B Tech / MCA / M-Tech • OEM (product quoted) Technical certification with prior experience of IT Infrastructure / Network Monitoring, enterprise level NMS and Helpdesk Management tools. • At least 5+ years of relevant experience in managing all aspects of IT/Network infrastructure and monitoring of the services in a large scale of network.	i. Overall System management at the Proposed Project Locations ii. Configuration and Administration of Servers and other hardware at the Proposed Project Locations. iii. Plan and liaise with vendors on maintenance work. iv. System issue troubleshooting
2.	BMS Specialist	• Diploma or equivalent with 8+ years' of experience including minimum 3-years' experience in Data Centre BMS environment.	i. BMS configuration and maintenance ii. Report Generation iii. Plan and liaise with vendors on maintenance work. iv. System issue troubleshooting
3.	Electrical Assistant	• Diploma in Electrical/ EEE or higher qualification with 4+ years' of experience including minimum 2-years' experience in Data Centre electrical environment, HT/LT Installation/ Maintenance.	i. Electrical Work for OSWAN NOC ii. Plan and liaise with vendors on maintenance work. iii. System issue troubleshooting

8. Service Level Agreement:

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the NIA to OCAC for the duration of this contract. The NIA and OCAC shall regularly review the performance of the services being provided by the NIA and the effectiveness of this SLA

For purposes of this Service Level Agreement, the definitions and terms as specified in the contract along with the following terms shall have the meanings set forth below:

- "Uptime" shall mean the time period for which the specified services / components with specified technical and service standards are available to OCAC or relevant user / beneficiary. Uptime, in percentage, of any component (Non IT & IT) can be calculated as: **Uptime = {1- [(Downtime) / (Total Time – Scheduled Maintenance Time)]} * 100**
- "Downtime" shall mean the time period for which the specified services / components with specified technical and service standards are not available to OCAC or relevant user / beneficiary and excludes the scheduled outages planned in advance for the NOC and the link failures that are OCAC's responsibility.
- "Incident" refers to any event / abnormalities in the functioning of the NOC Equipment / specified services that may lead to disruption in normal operations of the NOC services.
- "Helpdesk Support" shall mean the 24x7 on premise support centre which shall handle Fault reporting, Trouble Ticketing and related enquiries during this contract.
- "Resolution Time" shall mean the time taken in resolving (diagnosing, troubleshooting and fixing) an incident after it has been reported at the helpdesk. The resolution time shall vary based on the severity of the incident reported at the help desk. The severity would be as follows:
  - Critical: Incidents whose resolution shall require additional investment in components or time or shall involve coordination with OEMs. These incidents shall impact the overall functioning of the NOC. For example, purchase of printer, router, software bug fixing etc.
  - Medium: Incidents, whose resolution shall require replacement of hardware or software parts, requiring significant interruption in working of that individual component. For example, installation of operating system, replacement of switch etc.
  - Low: Incidents whose resolution shall require changes in configuration of hardware or software, which will not significantly interrupt working of that component. For example, installation of printer on a client etc.

8.1. Category of SLAs:

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The NIA shall

ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the NIA shall be reviewed by the OCAC that shall:

- Regularly check performance of the NIA against this SLA.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

8.2. Implementation Service Levels:

The following measurements and targets shall be used to track and report the implementation performance on a regular basis. The targets shown in the following table are applicable for the duration of the contract. All the targets for the completion of the implementation activity are calculated on a weekly basis. Please note that the Bidder should provide comprehensive, end-to-end service to implement the OSWAN-NOC Infrastructure, including replacement of the equipment in case of physical damage. No reason shall be entertained (unless those mentioned in Force Majeure) in case of unavailability of any service given in the scope of work in this RFP and the appropriate penalty shall be levied.

Measurement	Target	Severity	Penalty
Final Acceptance Testing	6 Months from the date of receiving the LoI	Critical	A Penalty as 1% per week for first two weeks, 2% per week for every subsequent week. Subject to maximum of 10%. Penalty will be computed on CAPEX value of contract.

8.3. Operations and Maintenance Service Levels:

Sr	Measurement	Target	Severity	Penalty
1	Individual Server Availability (including the OS, database and application running on it)	>= 99.982 %	Critical	No Penalty
		<99.982 %		1% of the QGR for every 1 hours of down time at a stretch or in-parts up to total down time of 10 hours. This to total down time of 10hours. This down time shall be calculated over and above the total hours of downtime permissible.

				Beyond 10 hours of down time, 2% of the QGR for every 0.5 hour of down time at a stretch or in parts.
2	NMS Reporting Availability	= 100%	Medium	No Penalty
		<100 %		1% of the QGR for every 1 hours of down time at a stretch or in-parts up to total down time of 10 hours. This to total down time of 10hours. This down time shall be calculated over and above the total hours of downtime permissible. Beyond 10 hours of down time, 2% of the QGR for every 1 hour of down time at a stretch or in parts.
3	Connectivity with Internet (With regards to equipment only)	>= 99.982 %	Critical	No Penalty
		<99.982 %		1% of the QGR for every 1 hours of down time at a stretch or in-parts up to total down time of 10hours. This to total down time of 10hours. This down time shall be calculated over and above the total hours of downtime permissible. Beyond 10 hours of down time, 2% of the QGR for every 0.5 hour of down time at a stretch or in parts.
4	Scheduled downtime for Preventive maintenance Per Week • 1am to 5pm on Sunday • Any further requirement for scheduled downtime as per approval from OCAC	Notification of >= 7 days in advance	Medium	No Penalty
		Notification of less than 7 days		0.5% of the QGR per incident

8.4. Physical Infrastructure Service Levels:

Sr	Measurement	Target	Severity	Penalty
1	UPS Availability (With regards to equipment only)	>= 99.982 %	Critical	No Penalty
		<99.982 % to >= 99.950 %		2% of the QGR
		>=98.00 % to <99.50 %		>=98.00 % to <99.50 %
		>=95.00 % to <98.00 %		8% of the QGR
		<95%		0.5% of the QGR for every 1 hours of down time at a stretch or in parts up to total down time in addition to the penalty mentioned above. This down time shall be calculated over and above the total hours of downtime permissible till 95.00 % availability.
2	Cooling system Temperature to be maintained 20°± 2° at all times Relative humidity to be maintained 50°± 5° at all times	>= 99.982 %	Critical	No Penalty
		<99.982 % to >= 99.950 %		2% of the QGR
		>=98.00 % to <99.50 %		>=98.00 % to <99.50 %
		>=95.00 % to <98.00 %		8% of the QGR
		<95%		0.5% of the QGR for every 1 hours of down time at a stretch or in parts up to total down time in addition to the penalty mentioned above. This down time shall be calculated over and above the total hours of downtime permissible till 95.00 % availability.
3	Surveillance: CCTV	>= 99.982 %	Critical	No Penalty

Sr	Measurement	Target	Severity	Penalty
	Availability would include DVR system availability, availability of CCTV recording	<99.982 % to >= 99.950 %		2% of the QGR
		>=98.00 % to <99.50 %		>=98.00 % to <99.50 %
		>=95.00 % to <98.00 %		8% of the QGR
		<95%		0.5% of the QGR for every 1 hours of down time at a stretch or in parts up to total down time in addition to the penalty mentioned above. This down time shall be calculated over and above the total hours of downtime permissible till 95.00 % availability.
4	Complete BMS system. This parameter applies to any individual component of BMS system, i.e., VESDA, Fire detection, fire suppression, WLD, Rodent repellent etc.	>= 99.982 %	Critical	No Penalty
		<99.982 % to >= 99.950 %		2% of the QGR
		>=98.00 % to <99.50 %		>=98.00 % to <99.50 %
		>=95.00 % to <98.00 %		8% of the QGR
		<95%		0.5% of the QGR for every 1 hours of down time at a stretch or in parts up to total down time in addition to the penalty mentioned above. This down time shall be calculated over and above the total hours of downtime permissible till 95.00 % availability.
5	NOC Infrastructure Management (Measure all the components at the end terminal level)	>= 99.982 %	Critical	No Penalty
		<99.982 % to >= 99.950 %		2% of the QGR
		>=98.00 %		>=98.00 % to <99.50 %

Sr	Measurement	Target	Severity	Penalty
		to <99.50 %		
		>=95.00 % to <98.00 %		8% of the QGR
		<95%		0.5% of the QGR for every 1 hours of down time at a stretch or in parts up to total down time in addition to the penalty mentioned above. This down time shall be calculated over and above the total hours of downtime permissible till 95.00 % availability.

8.5. Helpdesk Services:

Time in which a complaint / query is resolved after it has been responded to by the IT service management. In the Help desk Services SLA, if the NIA does not resolve any logged incident for more than the allowed resolution time, then the NIA is advised to escalate that criticality of the incident to next higher level.

Sr	Type of Incident	Target	Penalty
1	Incident logging	T = 5 minutes	No Penalty
		T1=T+5 Min	0.1% of the QGR for every late logging
		T2=T1+10 Min	0.5% of the QGR for every late logging
		>T2	2% of the QGR for every late logging
2	Assign/ Escalation	T = 5 mins.	No Penalty
		T1=T+5 Min	0.5% of the QGR for every late logging
		T2=T1+10 Min	2% of the QGR for every late logging

8.6. Compliance and Reporting Process Service Levels:

Sr	Measurement	Target	Severity	Penalty
1	Submission of MIS Reports. (The NIA shall submit the MIS reports as requested by OCAC)	Report for previous month to be submitted by 7 of next Month	Medium	1% of the QGR for every 1 day of delay in submission of incremental basis to a maximum of 5%
2	Implementing Change	100% of all approved	Medium	1% of QGR for >5

	Requests: The NIA would implement approved change request within 2 days of its approval	change requests		violations of Service Parameter
3	Customization of EMS reports	Customized reports shall be created and submitted within 7 days from date of request submitted by NIA.	Medium	1% of QGR for every 7 days delay in submission of customized reports to a maximum of 10% of QGR.

8.7. Manpower Resources Service Levels:

In cases where 24x7 man power is not available the support personnel should be available over phone. On critical situations or when directed by OCAC, the support personnel must be available on site within 3 hours of request from NIA. Non-availability of the support personnel as stated above will be treated equivalent to single occasion downtime for critical components. The manpower deployed by the NIA should be on rolls of the respective NIA and not contracted or outsourced personnel.

Sr	Measurement	Target	Severity	Penalty
1	Resource availability for all services requested under Operations and Maintenance. Resource availability would be calculated as: (No. of shift days for which resource present at the designated location / Total No. of shift days) x 100.	>= 99% averaged over all resources designated for System Integration (NOC Operations) services and calculated on a quarterly basis	Critical	No Penalty
		< 99% to >= 97% averaged over all resources designated for System Integration (NOC Operations) services and calculated on a quarterly basis.		2% of QGR
		< 97% to >= 95% averaged over all resources designated for System Integration (NOC Operations) services and calculated on a quarterly basis.		5% of QGR
		< 95% to >= 90% averaged over all resources designated for System Integration (NOC Operations) services and calculated on a quarterly basis.		8% of QGR
		< 90% averaged over all resources		Maximum penalty

		designated for System Integration (NOC Operations) services and calculated on a quarterly basis.		may be imposed i.e. 10% of QGR or on actual whichever is higher

Example: to illustrate the manpower availability in case there are there are 3 shifts per day which will have 2 people in shift 1, 1 in shift 2 and 1 in shift 3.
Total shift per day will be = 4 (2 x 1 + 1 x 1 + 1 x 1) per quarter it would be = 360 shifts
In a quarter if two people were not present in shift 1 for 7 days then, 2 x 7 = 14 shifts will be considered for the unavailability of manpower.
Uptime % = (shifts in which manpower was available / total number of shifts) x 100
Uptime = (1 — 14/360) x 100
Uptime % = 96.11%
Maximum penalty on manpower is limited to maximum of 10% of QGR. Manpower related penalty is additional to the penalty applicable for other services. Manpower related penalty will be either as per the SLA or as per actual rates of manpower absent during the quarter and the highest among these penalty will be applicable to the NIA.

8.8. SLA Review Process:

- Either OCAC or NIA may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.
- A meeting or conference call will be conducted to resolve the issue in a timely manner. The documented issues will be distributed to the participants at least 24 hours prior to the discussion if the issue is not an emergency requiring immediate attention.
- The OCAC and the NIA shall develop an interim solution, if required, and subsequently the permanent solution for the problem at hand. The NIA will then communicate the resolution to all interested parties.
- In case the issue is still unresolved, the arbitration procedures described in the Terms & Conditions section will be applicable.

8.9. Penalty Conditions:

- In O&M period, maximum of 10% Penalty will be computed on the value of QGR (exclusive of taxes) for a particular quarter.
- In the case of maximum Penalty of 10% being imposed on the NIA for two consecutive QGR, then the performance of the NIA will be reviewed and also may be subjected to cancellation of the order for failure of service level provided by the NIA or higher Penalty of 20% will be imposed on the NIA due to non-maintenance of Service levels.

9. General Terms and Conditions of RFP

Bidders should read these conditions carefully and comply strictly while submitting their bids.

9.1. Definitions

For the purpose of clarity, the following words and expressions shall have the meanings hereby assigned to them: -

a) “Request for Proposal (RFP)”, means this detailed notification seeking a set of solution(s), services(s), materials and/or any combination of them.
b) “OCAC”, shall mean the Odisha Computer Application Centre, the Designated Technical Directorate of Information Technology Department, Government of Odisha and OSWAN shall mean Odisha State Wide Area Network.
c) “GM” shall mean the General Manager of Odisha Computer Application Centre or any authorized officer to act on his behalf for a specified work.
d) “Authorized Representative” shall mean any person authorized by either of the parties.
e) “Agency/Vendor/Bidder/service provider” means any firm offering the solution(s), service(s) and /or materials required in the RFP. The word Agency/Vendor/Bidder/service provider when used in the pre award period shall be synonymous with Bidder, and when used after award of the Work shall mean the successful Bidder or Agency to whom OCAC issues the Purchase Order for rendering of sales & services.
f) "Service" means provision of Contracted service as per this RFP.
g) “Site” shall mean the location(s) for which the Order has been issued and where the service shall be provided as per Scope mentioned in the RFP.
h) “Termination Notice” means the written notice of termination of the Purchase Order issued by one Party to the other in terms hereof.

Note: *The bidder shall be deemed to have carefully examined the conditions, specifications, size, make and drawings, etc., of the goods to be supplied and related services to be rendered. If the bidder has any doubts as to the meaning of any portion of these conditions or of the specification, drawing, etc., he shall, before submitting the Bid refer the same to the procuring entity and get clarifications.*

9.2. Language

a) The Proposal should be filled by the bidders/Agency in English language only. For purposes of interpretation of the documents, the English translation shall govern. All Proposals and accompanying documentation will become the property of OCAC and will not be returned.
b) The Purchase Order as well as all correspondence and documents relating to the Project exchanged by the successful/ Agency and the Purchaser, shall be written in English language only. Supporting documents and printed literature that are part of

the Project may be in another language provided they are accompanied by an accurate translation of the relevant passages in the language specified in the special conditions of the contract, in which case, for purposes of interpretation of the Project, this translation shall govern.

c) The successful Bidder/Agency shall bear all costs of translation to the governing language and all risks of the accuracy of such translation.

9.3. Notices

a) Any notice given by one party to the other pursuant to the Project shall be in writing to the address specified in the Purchase Order. The term “in writing” means communicated in written form with proof of dispatch and receipt.

b) A Notice shall be effective when delivered or on the Notice’s effective date, whichever is later.

9.4. Governing Law

The Project shall be governed by and interpreted in accordance with the laws of the Govt. of Odisha/Govt. of India unless otherwise specified in the Purchase Order.

9.5. Project Value

a. The Project value (PO Amount) shall be paid as specified in the Purchase Order / Agreement subject to any additions and adjustments thereto, or deductions there from, as may be made pursuant to the Project.

b. Prices charged by the Supplier/ Agency(for the Goods delivered and the Related Services performed under the Project shall not vary from the prices quoted by the Supplier/ Agency in its bid, with the exception of any price adjustments authorized in the special conditions of the Project.

9.6. Recoveries from Supplier/ Agency

a) Recovery of liquidated damages, short supply, breakage, rejected articles shall be made ordinarily from bills.

b) OCAC shall withhold amount to the extent of short supply, broken/ damaged or for rejected articles unless these are replaced satisfactorily. In case of failure to withhold the amount, it shall be recovered from performance security deposit of AGENCY available with OCAC.

c) The balance, if any, shall be demanded from the Supplier/ Agency and when recovery is not possible, OCAC shall take recourse to law in force.

9.7. Taxes & Duties

a) The GST if applicable shall be deducted at source.
b) For goods/Equipment supplied from outside India, the successful/ Agency shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the country.
c) For goods/Equipment supplied from within India, the successful Agency shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Goods to the Purchaser.
d) If any tax exemptions, reductions, allowances or privileges may be available to the successful Agency in India, OCAC shall use its best efforts to enable the successful Agency to benefit from any such tax savings to the maximum allowable extent.

9.8. Insurance

The Agency should be responsible for undertaking comprehensive insurance including liability insurance, system and facility insurance and any other insurance for the personnel, Assets, data, software, etc relating to this assignment.

9.9. Transportation

The Agency shall be responsible for transport by sea, rail and road or air and delivery of the material in the good condition to the consignee at project locations. In the event of any loss, damage, breakage or leakage or any shortage the bidder shall be liable to make good such loss and shortage found at the checking/ inspection of the material by the consignee. No extra cost on such account shall be admissible.

9.10. Extension in Delivery Period and Liquidated Damages (LD)

a) Except as provided under clause “Force Majeure”, if the supplier/ selected bidder fails to deliver the related Services within the period specified in the Purchase Order, the Purchaser may without prejudice to all its other remedies under the Contract, deduct from the Purchase Order Price, as liquidated damages, a sum equivalent to the percentage specified in Section "Service Level Standards" for each week or part thereof of delay until actual delivery or performance, up to a maximum deduction of the percentage specified in the bidding document and/ or Purchase Order. Once the maximum is reached, the Purchaser may cancel the Purchase Order pursuant to clause “Termination”.
b) The time specified for delivery in the bidding document shall be deemed to be the essence of the Project and the supplier/ selected bidder shall arrange goods supply and related services within the specified period.
c) Delivery period may be extended with or without liquidated damages, if the delay in the supply of goods or service is on account of hindrances beyond the control of the selected bidder:
    I. The selected bidder/Agency shall request in writing to the Purchaser giving reasons for extending the delivery period of service, if he/she finds himself

/herself unable to complete the supply of goods or service within the stipulated delivery period or is unable to maintain prorate progress in the supply of goods or service delivery. This request shall be submitted as soon as a hindrance in delivery of goods and service occurs or within 15 days from such occurrence but before expiry of stipulated period of completion of delivery of goods and service after which such request shall not be entertained.

II. The Purchaser shall examine the justification of causes of hindrance in the delivery of goods and service and the period of delay occurred due to that and recommend the competent authority on the period of extension which should be granted with or without liquidated damages. Normally, extension in delivery period of service in following circumstances may be considered without liquidated damages:
    - When delay has occurred due to delay in approval by OCAC.
    - When the delay has occurred in providing space or any other infrastructure, if OCAC was required to provide the same as per the terms of the Bid.

III. If the competent authority agrees to extend the delivery period/ schedule, an amendment to the Purchase Order with suitable denial clauses and with or without liquidated damages, as the case may be, shall be issued. The amendment letter shall mention that no extra price or additional cost for any reason, whatsoever beyond the contracted cost shall be paid for the delayed supply of goods and service.

9.11. Termination

OCAC may at any time terminate the Purchase Order by giving written notice to the Bidder if the Bidder becomes bankrupt or otherwise insolvent. In this event, termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to OCAC. OCAC reserves the right to cancel the Purchase Order in the event of happening one or more of the following Conditions:

a) Failure of the successful bidder to accept the contract.
b) Delay in delivery beyond the specified period.
c) In addition to the cancellation of the contract, OCAC reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Bidder.
d) OCAC would not be liable to pay any damages to the Agency in cases comprising termination for default.

9.12. Settlement of Disputes

a) General: If any dispute arises between the supplier/ Agency and OCAC during the execution of a Project that should be amicably settled by mutual discussions. However, if the dispute is not settled by mutual discussions, a written representation will be obtained from the supplier/ Agency on the points of dispute. The representation so received shall be examined by the concerned Committee which sanctioned the tender.

The Procurement Committee may take legal advice of a counsel and then examine the representation. The supplier/ Agency will also be given an opportunity of being heard. The Committee will take a decision on the representation and convey it in writing to the supplier/ Agency.

b) Standing Committee for Settlement of Disputes: If a question, difference or objection arises in connection with or out of the Order issued or the meaning of operation of any part, thereof or the rights, duties or liabilities of either party have not been settled by mutual discussions or the decision of tender sanctioning Procurement Committee, it shall be referred to the empowered standing committee for decision.

10. Special Terms and Conditions of RFP

10.1. Support

a) The bidder must execute back to back support contract with OEM for the period of Five Years from the date of UAT.
b) The Agency shall either repair or reinstall the corrupt s/w or parts thereof with brand new genuine/ authentic ones having similar or higher specifications from the respective OEM as per the time period specified.

10.2. Roles and Responsibilities Matrix

The roles of the stakeholders shall change over a period of time as the project will evolve from design to implementation phase only. Below mentioned Table summarizes the roles and responsibilities of key resources of stakeholders involved in the project.

Role	Responsibility Centre	Roles and Responsibility
Implementation Agency Project Leader	OCAC	• Shall spearhead the coordination strategy for the project across all stakeholders. • Shall have the authority to approve deliverables, release circulars/notifications • Shall coordinate with the Project Management Unit to finalize a comprehensive reporting framework which shall cater to various stakeholders especially decision makers for supervising implementation. • Shall ensure compliance to the specifications defined in the area of application design, infrastructure and management. • Head the Change Approval Board and provide the final approval for any project related changes that have to be performed during

Role	Responsibility Centre	Roles and Responsibility
		development and maintenance phases • Monitor and review the success of the system and ensuring its effective and efficient running. • Maintain daily, weekly and monthly reports for the same for higher management. • Work in connection with other IT experts in the organization. • Address key security and privacy requirements for secure business solutions. • Provide extensive technical, strategic advice and guidance to the System Integrator/NIA for proper implementation. • Act as an active member of the CAB and provide technical inputs on IT related changes in the software. Identify and highlight potential risks.
Implementation Agency (IA)	NIA	• Run the project from design and development to implementation. • Define requirements and plan project lifecycle for deployment. • Define resources and schedule for the project's implementation. • Create strategies for risk mitigation and contingency planning. • Plan and schedule project deliverables, goals, and milestones • Direct and oversee project implementation team. • Efficiently identifies and solves project issues. • Design and maintain technical and project documentation. • Act as an active member of the Change Approval Board (CAB) and highlight any risks / issues that could take place in the software system if a particular change is implemented. • Co-ordinate with the team members for effective delivery.

Role	Responsibility Centre	Roles and Responsibility
		• Communicate with the Project Management Unit • The IA shall be responsible for managing the computers, network and other infrastructure facilities required for the project. • The IA should maintain backup of digital content after user acceptance. • The IA shall be responsible of implementation of NMS & Ticket Management. • This team will support the System Administrator at OCAC for all technical issues.
Non IT Infrastructure Team	NIA	• This team would be responsible for the design, development, installation, configuration of the OSWAN NOC • Maintain technical documentation for the installed components in the NOC
Third Party Audit	TPA	• Ensure compliance to the requirements of OSWAN-NOC as per Agency the clauses of the RFP, information security guidelines, interoperability standards, data storage requirements and business continuity principles. • Assess technology obsolescence risk and propose technology risk mitigation plan. • Validate the delivery and installation schedule and commissioning plan. • Perform the FAT and ensure Go-Live • Ensure that the SLA reports are validated and suggest the liquidated damages / penalty to be deducted from the QGR • Shall validate all the invoices before forwarding to OCAC for approval and payment.

10.3. OCAC Obligations

OCAC will facilitate all necessary space, raw power arrangement (up to transformer) and necessary approvals for implementing the OSWAN-NOC. The NIA needs to liaison with OCAC for all necessary approvals. OCAC will facilitate and co-ordinate to liaison with other stakeholders such as OSWAN Operator, HOSWAN Operator, Bandwidth

Provider etc. Any delay for implementation which is not attributable to NIA shall be reported by the NIA in writing immediately so that OCAC may record the cause of the delay and take necessary actions. OCAC will provide comments or approvals for the documents or reports submitted by the NIA in a timely manner for smooth execution of the project.

10.4. Payment Terms and Schedule

Payment terms regarding supply, installation and commissioning of OSWAN-NOC infrastructure (including all civil, IT and Non-IT assets)

- Payment towards installation and commissioning would be made only upon successful completion of PAT for the assets.
- Payment towards assets may be released on pro-rata basis during FAT / Go-live sign off.
- All payments would be made on the basis of milestone completion only. No pro-rata payment would be entertained to the bidder under any circumstances.
- All payments would be done after evaluation and approval of the Payment Approval Committee (PAC) constituted by OCAC within 30 days from the date of submission of invoice. Any dispute / discrepancy around the invoice needs to be raised within 20 days of the invoice submission.
- All invoices should be submitted in triplicate copies.

Sl No	Activity	Payment	Remarks
1	Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval	70% of the quoted CAPEX cost for the activity (Non-IT Infrastructure works)	Submission of design documents, layout, drawing etc. For statutory approvals.
2	Finalization and Approval of the submitted layout, Floor diagram, Non-IT and IT architecture, etc.		OCAC has to approval of submitted drawings and layout.
3	Completion of Structural, Architectural, Civil & Interior Work		Completion of all Civil and Interior works and inspection report of all item delivered & erected. Successful bidder shall furnish weekly progress

			report.
4	Supply of all Non-IT asset.(excluding the civil and interior works)		Successful bidder shall share all itemized delivery details and challans related to the assets. OCAC will verifying the supply & sign-off of Non-IT Infrastructure.
5	Installation and Commissioning & Testing of all Non-IT asset.	20% of the quoted CAPEX cost for the activity (Non-IT Infrastructure works)	Successful bidder shall carry out integrated system testing of all equipment and rectify all snags and get acceptance Test sign-off of Non-IT Infrastructure system from OCAC
6	Supply of all IT asset	60% of the quoted CAPEX cost by the bidder for IT Infrastructure	Successful bidder shall share all itemized delivery details and challans related to the assets. OCAC will verifying the supply & sign-off of Non-IT Infrastructure.
7	Installation and Commissioning of all IT asset	30% of the quoted CAPEX cost by the bidder for IT Infrastructure	Successful bidder shall carry out integrated system testing of all equipment and rectify all snags and get acceptance Test sign-off of IT Infrastructure system from OCAC
8	Project Sign-Off & FAT (Go-Live of the Project)	Rest Payment = (10% of the quoted CAPEX cost by the bidder for IT & Non-IT Infrastructure - Penalty)	Successful Final Acceptance Test of all commissioned IT and Non-IT systems and Issue Go-Live Certificate from OCAC
9	Operations and maintenance cost including Manpower cost	Quarterly O&M payment = (Yearly OPEX Cost /4 - Penalty)	Operations and Maintenance cost including Manpower cost submitted by the bidder to be distributed uniformly into entire Project periods.

10.5. Payment of Goods & Services Tax

GST shall be shown extra by the bidder in their invoices for the items applicable. The same shall be paid by OCAC as per actual after verification If there is any tax savings, the same shall be reduced from the payable amount. In case of any new incidence of tax or increase in existing tax rates taking place during the Project Period, that shall be borne and payable by the OCAC over and above the agreed price for each item as may be

applicable as per the Invoice raised by the agency on the OCAC. Similarly, any reduction in taxes shall be to the benefit of OCAC.

10.6. Implementation Schedule

Week	Activity	Remarks
S + 0	Project Implementation Kick-off by NIA	This would be done within 1 week of award of contract.
S + 4	Preparation & Submission of OSWAN-NOC Layout	The NIA shall design the OSWAN-NOC layout in consultation with the OCAC team
S + 5	Approval of the Layout	OCAC shall approve the layout before NIA start their Non-IT infrastructure work
S + 6	OSWAN-NOC Design & approval	The NIA shall design the OSWAN-NOC technical (IT) blueprint in consultation with the OCAC team. OCAC shall approve the layout before NIA start their Non-IT infrastructure work
S + 12	Civil construction as required for NOC area & Civil and interior installation activities	NIA shall carry out interior Civil work as required to complete the civil work required for OSWAN-NOC. Also all the minor civil work like internal painting, tiles work, false flooring, false ceiling, civil work for installation of doors, partitions, AC's etc. will be carried out by NIA at this stage.
S + 30	Commissioning of NOC	While non-IT components will be installed, PAT for Non-IT components will be carried out by the OCAC. On acceptance of Non-IT implementation, IT components will be delivered and implemented. PAT for IT components will be carried out once the commissioning of IT components done.
S+ 36	Final Acceptance Tests & Go-Live	OCAC shall draft the FAT checklist. Final Acceptance Test will be carried out by NIA in the presence of OCAC with reference to implementation of OSWAN-NOC infrastructure. On satisfactory acceptance by OCAC the NIA shall start the O&M phase

Note: - S=1 week from the date of issue PO/LoI.

11. MINIMUM TECHNICAL SPECIFICATIONS

11.1. Tentative Bill of Materials for OSWAN-NOC:

The tentative bill of material is mentioned below. However, if the bidder will go with separate solution beyond the BoQ mentioned, S/he has to submit the separate BoQ, matching with all Technical specification mentioned in clause 11.2 to 11.3.13.

Sl No	OSWAN-NOC Components	Unit	Qty
IT Infrastructure			
1.	Rack Mount Server	No's	5
2.	SAN Storage – 20 TB usable and scalable upto 100TB	No's	1
3.	SAN Switch - 24 ports scalable up to 48 ports	No's	2
4.	DMZ Switch	No's	2
5.	24 port L3 Network Switch	No's	2
6.	Access PoE Switch	No's	4
7.	**NMS, Automation & Helpdesk Management System for OSWAN Equipment**	Set	1
a.	IT Network Discovery & Monitoring		
b.	NMS Server Infrastructure Monitoring		
c.	IT Network Fault Management		
d.	IT Performance Management		
e.	IT Service Management		
f.	IT Network Performance Management		
g.	Reporting and Dashboards		
h.	Automation		
i.	User Interface, User Authentication & Authorization, User Administration & User Audit		
8.	Backup Software	Set	1
9.	Backup Appliance with 16 TB usable capacity	Set	1
10.	Virtualisation Software	As Required	10
11.	One time implementation and upgradation cost of existing setup	Set	-
12.	Windows Server OS Standard Edition (Latest version) as per Bidder's solution	As Required	
13.	Linux Server OS Enterprise Edition (Latest version) as per Bidder's solution	As Required	
14.	Enterprise Analytical Database as per Bidder's solution	As Required	
15.	Server Security solution (HIPS) Licences, as per Bidder's solution	As Required	
16.	Desktop with Preloaded Windows & MS Office (latest version), Antivirus	No's	3
17.	Multifunctional Printer	No's	1
18.	Any Other IT components (please specify)		
Non- IT Infrastructure			

Sl No	OSWAN-NOC Components	Unit	Qty
1.	Civil & Interior Works (Including Dismantling & Construction of Brick work, masonry work, painting, Partition, False floor, Raised Floor, False ceiling, Water proofing, etc.	Set	1
2.	Electrical System Works (Including electrical panel, Earthing, NOC internal electrical wiring, DB, Switchgears, Lighting & fixtures, etc for all NOC Areas, DC Areas, Helpdesk Areas & Office Areas)	Set	1
3.	Portable Server Firm enclosure with minimum 12 racks (6 Server Racks & 6 Network Rack). The enclosure should at least be built in with 1. Precision Air Conditioner (4 X 20 Kw) with N+1 architecture to maintain a temperature of 22 degree centigrade with variation of +/- 2 degree and 50% +/-5RH. 2. Fire Detection and Suppression system using Novec 1230 Gas 3. Security & Surveillance System 4. Rodent repellant System 5. Access Control System (Biometric access control system which should be control by access control panel) 6. WLD 7. Intelligent Rack PDU (Vertical, 0U), Metered, 32 A, Single Phase, minimum IEC 320 C13 x 24 and IEC 320 C19 x 6 output sockets, each rack should have two iPDU's 8. Electrical fitting 9. Any other component required for a Data Centre	No's	2
4.	Video Wall (3x2) with Controller and accessories	Set	2
5.	Passive Networking (including Cat-6 Cable, Patch panel, MPO cassettes, Cable basket, Fibre Runner, I/O module, Patch Cord-Copper/Fiber, Faceplate, Wall mount Rack, Conduit with accessories)	Set	1
6.	UPS of 40 KVA with each 30 Minutes backup. The UPS system should also have provisioning of adding one more 40 KVA system to work in N+N / N+1 architecture.	3	Nos.
7.	Setting up of Network Operation Centre As per SoW		
8.	Any Other components (please specify)		
9.	IP KVM switch	Set	1
Implementation & Training			
1.	Non-IT Infrastructure Implementation	Lot	1
2.	IT Hardware Infrastructure Implementation	Lot	1
3.	NMS, Automation & Helpdesk Management System Implementation & Training	Lot	1

Note: Bidder has to submit Bill of material as per their solution. The Bidder has to mention each component individually in the BOQ and unit price for every component in the

commercial bid. The bidder has to ensure 5 years comprehensive onsite and back to back support from OEMs for all the items quoted by the bidder.

11.2. Non- IT Infrastructure Technical Specifications:

All the specifications and requirement mentioned below are indicative and bidder may propose their own design and architect for the OSWAN-NOC site.

11.2.1. Rack Placement Details (MDC @SHQ)

- Total 6 Server Racks and 6 Network Racks along with Air Conditioner will be placed in the Portable prefabricated Server Farm.
- Server Rack Size will be 600mm X 1000mm
- Network Rack - 2 / 4 Post Open Rack with vertical Wire Managers
- Cabling requirement for respective racks.
- Intelligent Rack PDU (Vertical, 0U), Metered, 32 A, Single Phase, minimum IEC 320 C13 x 24 and IEC 320 C19 x 6 output sockets , each rack should have two iPDU's.

11.2.2. Civil and Architectural Work

The scope for civil work in this RFP is to furnish the area of Portable Server Firm enclosure and operation centre in all aspects. The furnishing includes but not limited to the following

- Cement Concrete Work
- Cutting and chipping of existing floors
- Trench works (if required)
- Masonry works
- Hardware and Metals
- Glazing
- Paint work
- False Ceiling
- Storage
- Furniture & fixture
- Partitioning
- Doors and Locking
- Painting
- Fire proofing all surfaces
- Insulating

11.2.3. Civil Work (If Required)

- Providing and laying 115 mm thick brick work in cement mortar of 1:4 (1 cement: 4 sand) with bricks of approved quality chamber bricks of class designation 50.
- Providing & making SS signage with text in etched & black painted to be located as directed (wall mounted) for space nomenclature/ directions.
- Plastering with cement mortar 1:5 (1 cement : 5 sand) of 12 mm thick in interior face of the walls and concrete columns including hacking the concrete surface brushing, scaffolding, curing and surface shall be smooth trowel finish as per standard specification.
- Anti-termite treatment of the entire critical area.

11.2.4. Painting

- Providing and applying Fire retardant paint of approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint.
- For all vertical Plain surface.
- For fire line gyp-board ceiling.
- Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.
- Applying approved fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.

11.2.5. False Ceiling

- Providing and fixing metal false ceiling with powder coated 0.5mm thick hot dipped galvanised steel tiles 595 x 595 mm with tegular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanised steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles and 25mm thick glass wool of 16kg.sq.m density wrapped on both sides with aluminium foil and placed over each tile etc.
- Providing and fixing 12 mm thick fire line Gypsum false ceiling and lighting troughs 300 mm as per design including 100 mm high cornices as lighting pelmets on G.I. frame work, in G.I. vertical supports at every 450mm c/c and horizontal runners at every 900mm c/c self taping metal screws to proper line and level. The same shall be inclusive of making holes and required framing for fixing electrical fixtures, A.C. grills etc. Area of electrical fixtures will be

paid full fixed to G.I. supports to receive spotlights including cutting hole etc., complete. G.I. metal frame to be of 24 gauge folded strip of 50mm width to be used. GI vertical supports to be anchored to slab by means of anchor fasteners.

11.2.6. Furniture and Fixture

- Workstation size of 2' depth made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc complete with French polish. The desk top will be 25mm thick & edges shall be factory post formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per design, complete with approved quality drawer slides, hinges, locks etc.
- Providing & making of storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate color out side and 2 coat of enamel paint inside the storage of size 1'6"x1'9"x2'4". The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with French polish
- Cabin table of depth 2’ made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc complete with French polish.
- Providing, making & fixing 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low ht partition, brick wall, partition wall, cladding etc complete with French polish in all respect.
- Providing, making & fixing an enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate color out side and 2 coat of enamel paint inside the shutter. The same should be provided with all the required accessories including the handle, lock, loaded hinges, tower bolt and necessary hardware etc. complete with French polish.
- Fire proof safe (150 Ltrs. or above) with one hour fire rated.

11.2.7. Partitions (If Required)

- Providing and fixing in position full height partition wall of 125 mm thick fireline gyp-board partition using 12.5 mm thick double fireline gyp-board on both sides with GI steel metal vertical stud frame of size 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition. Glass wool insulation inside shall be provided as required. Fixing is by self tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cutouts for switch board, sockets, grill etc. It shall also

include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire resistant coating.

- With glazing including the framework of 4" x 2" powder coated aluminium section complete (in areas like partition between server room & other auxiliary areas).
- Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this)
- All doors should be minimum 1200 mm (4 ft) wide.

11.2.8. PVC Conduit

- The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for non-metallic conduit 1.6 mm thick as per IS 9537/1983.
- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.
- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed.
- All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw and junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.
- Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.
- The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.

11.2.9. Wiring

PVC insulated copper conductor cable shall be used for sub circuit run from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Color code for wiring shall be followed.

- Looping system of wring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations. No wire smaller than 3.029 sq.mm shall be used.
- Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.
- Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.
- All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.
- Metal clad sockets shall be of dia cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.
- All power sockets shall be piano type with associate’s switch of same capacity. Switch and socket shall be enclosed in a M. S. sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.
- Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts The earth continuity insulated copper wire in Green color

shall be run inside the conduit to earth the third pin or socket outlets, earth terminal of light fixtures, fan etc. as required. Lights points shall be either of single control, twin control or multiple points controlled by a single switch / MCB as per scheduled of work. Bare copper wire shall be provided with each circuit from DB as specified in the item of work and terminated in earth bar of DBs and switch boxes with proper lugs as required maximum number of PVC insulated 650 / 1100 grade copper conductor cable which can be drawn in a conduit

11.2.10. Earthing (MDC, PAC, UPS)

Three separate earthing will be done for Modular DC, PAC & UPS System. All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. Earthling shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS- 3843. The entire applicable IT infrastructure in the Data Center shall be earthed.

- Earthing should be done inside the identified area for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, and AC units etc. so as to avoid a ground differential.
- State shall provide the necessary space required to prepare the earthing pits.
- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
- The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.
- Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.
- The Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself in the UPS room.
- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.
- The earth connections shall be properly made .A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lighting surge, high voltage surge or failure of bushings.

- The SELECTED BIDDER would be responsible for providing separate Earthing for Servers, UPS & Generators as per the standards.

11.2.11. Cable Work

- Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a crisis crossing is avoided and final take off to switch gear is easily facilitated.
- All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick aluminum strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.
- Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.
- Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.
- Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.
- Necessary earthling arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.
- The space between data and power cabling should be as per standards and there should not be any criss-cross wiring of the two, in order to avoid any interference, or corruption of data.

11.2.12. Uninterrupted Power Supply (UPS) SYSTEM:

- Supply, installation, testing and commissioning of true online, double conversion, > 94% overall efficiency, and high-power factor Uninterruptible Power Systems (UPS) rated at 40 kVA with battery backup support for 30 minutes with each UPS System on full load. UPS shall be rack mounted &

the backup batteries should be supplied with the necessary arrangements for external mounting.

- Configuration: 3 x 40 kVA (True online, IGBT based, Dual Conversion). Should have the provision to add one or more same capacity UPS in parallel (N+1).
- All Server racks will get power feed from two independent UPS systems to ensure redundancy.
- Battery & UPS should be mounted outside of the considered DC area.
- Scope includes battery bank connections and providing safety barriers for all bus bars and cable connection leads on battery racks.

Make **Model**				
SL. NO.	**PARAMETER**	**SPECIFICATION**	**Compliance (Yes/No)**	**Pg.No. of Tech. Specs attached**
1.1.	UPS type	ON-LINE, Rack mountable		
1.2.	Input Ratings			
1.2.1.	Nominal Input	Voltage, Range 415V AC (3-Phase), 340 V – 480 VAC		
1.2.2.	Nominal input frequency	50 Hz		
1.2.3.	Input power factor at full load	> 0.99 at full load		
1.3.	Out Put Ratings			
1.3.1.	Nominal output voltage	380V / 400V (3-phase)		
1.3.2.	Output Voltage regulation	< +/- 1%		
1.3.3.	Output voltage distortion	<2% THD maximum for 100% linear load.		
1.3.4.	Nominal output frequency	50 Hz		
1.3.5.	Power factor	0.9 lagging		
1.3.6.	Over load capability	125% for 5 minutes, 150% of full load for 1 minute		
1.4.	Battery Parameters			
1.4.1.	Type	12V, SMF		
1.4.2.	Make	Exide/Rocket/ Amaron Quanta		
1.4.3.	Minimum VAH for 30 min. back up	38400 VAH with each UPS System. ***Note: Any defective battery needs to be replaced by the bidder, during project period, as and when required. Also, the bidder needs to replace entire battery unit for 1 time in entire project period.***		
1.5.	Environmental Parameters			
1.6.	Operating temperature	0 to 40 deg. Centigrade		
1.7.	Relative	95% RH non-condensing		

Make Model				
SL. NO.	**PARAMETER**	**SPECIFICATION**	**Compliance (Yes/No)**	**Pg.No. of Tech. Specs attached**
	Humidity			
1.8.	Altitude	1000 meters		
1.9.	Noise level	<58db		
1.10.	Remote Monitoring Software	SNMP& MODBUS to be provided for remote monitoring & BMS.		

11.2.13. Precision Air Conditioning

The Portable prefabricated server firm shall be provided with fully redundant Precision Air-conditioning system. A/C should be capable of providing sensible cooling capacities at design ambient temperature & humidity with adequate airflow. The PAC should be capable to be integrated with the Building management System for effective monitoring.

The PAC should be step less variable capacity cooling, horizontal Throw unit complete with Compressor, green Refrigerant, outdoor unit, heater, humidifier, rated for actual cooling capacity @ 32 Deg C return air temp. suitable to give 21+/-1 Deg. C in Cold aisle at 37 deg C ambient condition.

The Agency will be required to design, supply, transport, store, unpack, erect and test the successful commissioning and satisfactory completion of trial operations of the PAC systems for the room and Portable Server Firm Enclosure . This shall also include-

- Connecting the indoor unit with the mains electrical point
- Connecting indoor and outdoor units mechanically (with 18 G hard Gauge Copper piping).
- Connecting indoor and outdoor unit electrically.
- Nitrogen pressure testing, triple vacuum, final gas charging.
- Connecting the humidifier feed line with the point provided.
- Connecting the drain line with the point provided.
- Commissioning and handing over the unit to the customer.
- Operation and routine maintenance training to up to two persons nominated by the customer while commissioning the units at site

This PACs should be as per N+1 or N+N redundancy requirement.

11.2.14. Temperature Requirements:

The environment inside the room and Portable Server Firm Enclosure at OCACshall need to be continuously maintained at 22 ± 2^{o}Centigrade. It is advised that the temperature and humidity be controlled at desired levels. The necessary alarms for variation in temperatures shall be monitored on a 24x7 basis and logged for providing reports.

11.2.15. Relative Humidity (RH) requirements

Ambient RH levels shall need to be maintained at 50% ± 5 non-condensing. Humidity sensors shall be deployed. The necessary alarms for variation in RH shall be monitored on a 24x7 basis and logged for providing reports.

11.2.16. Temperature & Relative Humidity Recorders

Temperature and Relative Humidity Recorders shall preferably be deployed for recording events of multiple locations within the room and Portable Server Firm Enclosure at OCAC. Records of events for about past 7 days shall be recorded and presentable whenever required by OCAC.

11.2.17. Air quality levels

The room and Portable Server Firm Enclosure shall be kept at highest level of cleanliness to eliminate the impact of air quality on the hardware and other critical devices. The room and Portable Server Firm Enclosure shall be deployed with efficient air filters to eliminate and arrest the possibility of airborne particulate matter which may cause air-flow clogging, gumming up of components, causing short-circuits, blocking the function of moving parts, causing components to overheat etc. Air filters shall be 95% efficiency & provide up-to 5 Micron particulate shall be deployed

11.2.18. Additional Points

- The precision air-conditioners should be capable of maintaining a temperature range of 22 degree with a maximum of 2 degree variation on higher and lower side and relative humidity of 50% with a maximum variation of 5% on higher and lower side.
- The unit casing shall be in double skin construction on the side panels and single skin on the front & back panels for longer life of the unit and low noise level.
- For close control of environment conditions (Temp. and RH) the controller shall have (PID) proportional integration and differential.
- The precision unit shall be air cooled refrigerant based system to avoid chilled water in critical space.

- The internal rack layout design shall follow cold aisle and hot aisle concept as recommended by Ashrae.
- The refrigerant used shall be environment friendly R-410-A in view of long term usage of the data centre equipments, availability of spares and refrigerant.
- The fan section shall be designed for an external static pressure of 25 Pa.
- Microprocessor Controls: Following features should be displayed on the units
  - Room temperature and humidity.
  - Humidifier working status
  - Manual / Auto unit status
  - Temperature set point
  - Humidity set point
  - Working hours of main component i.e. compressors, fans, heater, humidifier etc.
  - Unit working hours
  - Current date and time
  - Type of alarm (with automatic reset or block)
  - The last 10 intervened alarms
- The microprocessor should be able to perform following functions
  - Testing of the working of display system
  - Password for unit calibration values modification
  - Automatic re-start of program
  - Compressor starting timer
  - Humidifier capacity limitation
  - Date and time of last 10 intervened alarm
  - Start / Stop status storage
  - Random starting of the unit.
  - Outlet for the connection to remote system
  - Temperature and humidity set point calibration
  - Delay of General Alarm activation
  - Alarm calibration
- Following alarms shall be displayed on screen of microprocessor unit:
  - Air flow loss
  - Clogged Filters
  - Compressor low pressure
  - Compressor high pressure
  - Smoke - fire
  - Humidifier Low water level
  - High / Low room temperature
  - High/Low room humidity
  - Spare External Alarms
  - Water Under floor
  - The control system shall include the following settable features:

- Unit identification number
- Startup Delay, Cold start Delay and Fan Run on timers
- Sensor Calibration
- Remote shutdown & general Alarm management
- Compressor Sequencing
- Return temperature control
- Choice of Modulating output types

- The unit shall incorporate the following protections:
  - Single phasing preventers
  - Reverse phasing
  - Phase misbalancing
  - Phase failure
  - Overload tripping (MPCB) of all components

11.2.19. Racks & Accessories

Supply and installation of IT Rack with containment, having 42U as standard, complete with cable manager & blanking panels with iPDU and rack accessories. Racks to made out of quality CRCA offering highly rigid and stable structure for loading per rack up to 1000 KG .

- Multi fold heavy duty 19” mounting rails in the IT rack should be made from 2.0mm CRCA ensure rigidity and load carrying capacity while maintaining the overall squareness of the structure.

- Pairs of mounting rails of IT racks should have two mounting webs for the ease of mounting 19” equipment and accessories like shelves, chassis runners etc. These rails should be fully adjustable and should offer operational flexibility while setting up the rack for installations.

- The 19” Mounting rails should recess throughout the depth of the rack.

- Rack design should offer access for the entire rack configuration from inside the rack which will eliminates the need for access from the side of the rack. In the event of a complete row of racks – each rack can be changed in to its configuration independently without taking it out from the row since side access is not required for re-orient the rack internally. (e.g. Moving vertical mounting rails to accommodate different size of rack mounted device.)

- The Roof of the rack should have multiple gland plates which can be used for cable entry and / or mounting the fan trays.

- Doors and panels of racks should be removable type. Every door should open 180 degrees –for the ease of servicing the rack after installation and / or mounting / removing the equipment. Rear door should be in split design.

- Side panels should be lightweight and easily removable type with pair of spring latches. Lock should be provided for making the rack completely secured.

11.2.20. Cold Aisle Containment

Supply and installation cold aisle containment for data centre infrastructure with following technical specification & features:

- The Cold Aisle containment should be constructed between two symmetrical rows of racks facing each other in Cold Aisle.
- The Cold Aisle containment should be modular to enable to add the racks.
- All the components used in the Aisle containment shall be Fire Retardant.

11.2.21. Entry Doors of Containment:

- Entry and Exit Doors of the Cold Aisle should have open able or sliding double door
- Each door should have CRCA frame with fire retardant glass sheet of 4 mm thick or Fire Retardant Rigid UL V-0 Plastic 3 mm
- The frame of door should have 4 vertical MS Columns of rectangular section with thickness of 1.5mm
- 4 columns should be grouted to real floor or can be fixed to the base frame of rack
- Vertical columns should be connected to each other with help of Cross members. These Cross members should be length of Cold Aisle width
- The Doors must have a Steel Picture Frame fabricated in 1.2mm thick CRCA sheet as per “IS 513 Grade D” standards
- PU Foam Gasket should used across the metal edges of the door to prevent any leakage on cold air
- The doors should have automatic door closers installed to ensured that those are closed.
- Polyamide Cable Brushes should be fitted at the bottom of doors to avoid leakage of cold air when doors are closed.
- Top panels of the cold aisle should be covered with either fire rated Glass or Polycarbonate panels
- Top Panels are fixed in CRCA frame per “IS 513 Grade D” with thickness of 1.2 mm
- The Glass/ Polycarbonate in the top Panels are of 4 mm thick
- Top Panel must be tool less installation to offer quick access to area above the contained aisle during the maintenance activity
- Top Panel must have opening for Smoke Sensor/ FM System wherever necessary Powder Coating
- The Powder coating complies with ROHS requirement to avoid hazardous substance contamination in the Data Center. Pre-treatment Nano Ceramic process should be followed.
- The powder coating thickness is 80-100 Microns

11.2.22. Intelligent Rack PDU

Supply, Installation, Testing & commissioning of Intelligent Rack PDU (Vertical, 0U), Metered, 32 A, Single Phase, minimum IEC 320 C13 x 24 and IEC 320 C19 x 6 output sockets , each rack should have two iPDU's with following specification :

- Input current rating: 230V, 1-ph, 32A
- It should have billing grade +/-1% Accurate Metering of electrical parameters as per ANSI Standards
- It should have min. 2 nos of 100% rated Low Profile magnetic hydraulic circuit breaker for single phase iPDU
- It should conform to UL/CE, IEC Norms
- All plug types, input as well as outlet should confirm to best industry standards and should have locking capability to avoid accidental dislodging.
- Locking Capability should be Inbuilt to the Sockets to make use of normal Cables. In case, special power cords are required, it should be supplied by the bidder with PDUs.
- Sockets should be preferably coloured to clearly identify different circuits
- It should support High Operating temperature of 0 to 60 deg C to take care of high operating temperature at back of Rack
- It should provide following measurement parameters at rack level: Current (A), voltage (V), real power (W), apparent power (VA), consumption (kWh) and power factor
- iPDU should have capability to Daisy Chain min 16 iPDUs to reduce use of number of Network Ports usage. During Daisy Chaining each PDU should retain its own IP Address for easy identification and Mapping and should maintain high availability over network.
- The iPDU should have dual Ethernet Ports.
- Provided Solution should have capability for Simultaneous Commissioning, Updating Firmware, Setting Thresholds and Alarms across Multiple iPDUs using a centralized software
- Communication module in the rack PDU should be Hot Swappable.
- The iPDU should support an Android or iOS app for easy read of PDU recorded Power readings. The Connection should not use Bluetooth to prevent breach.

- For Security iPDU should support encryption via TLSv1.2
- Should provide Ease of integration into third party systems supporting an API
- It should be integrated with OEM's IT management software or DCIM
- It should have lowest power consumption about 10W on idle.
- The communications protocols supported should include:

  ARP, IPv4, IPv6, ICMP, ICMPv6, NDP, TCP, UDP, DNS, HTTP, HTTPS, SMTP, SMTPS, DHCP, SNMP (v1/v2c/v3), and Syslog.

- It should have adjustable threshold values with an alarm function
- PDU should provide the capability of reporting error thru email or any other method suitable
- iPDU should have capability to connect up to 16 sensors (temperature, humidity, airflow, door contact, Dew Point).
- It should have USB port for firmware upgrade and external log storage.

11.2.23. Comfort Air Conditioning for Auxiliary Areas

- Capacity – minimum 6.0 Tonnage
- Cooling Capacity – minimum 24000 BTU / Hr
- Compressor – Hermetically Sealed Scroll Type
- Refrigerant – R 22 Type
- Power Supply – Three Phase, 380-415 V, 50 Hz
- Air Flow Rate – minimum 19 cu m / min
- Noise Level - < 50 dB
- Operation – Remote Control

11.2.24. Fire Detection and Control Mechanism

Fire can have disastrous consequences and affect operations of a Data Center. The early-detection of fire and employing means for automatic suppression of the fire is important for effective functioning of room and Portable Server Firm Enclosure.

11.2.25. System Description:

- The Fire alarm system shall be an automatic 1 to n (e.g. 24) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.

- Detection shall be by means of automatic heat and smoke detectors to be installed in MDC (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.

11.2.26. Control and indicating component

The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply.

- All controls of the system shall be via the control panel only.
- All site-specific data shall be field programmable and stored in an integral EEPROM. The use of EPROM's requiring factory 'burning' and reprogramming is not acceptable.
- All internal components of the control panel shall be fully monitored.
- The control panel shall be capable of supporting a multi device, multi zone 2-wire detection loop. Removal of 1 or more detection devices on the loop shall not render the remaining devices on the loop inoperable.
- The system status shall be made available via panel mounted LEDs and a backlit alphanumeric liquid crystal display.
- All user primary controls shall be password protected over 4 access levels in accordance with EN54 Part 2. Essential controls, such as Start / Stop sounders and Cancel fault buzzer, etc. will be clearly marked.
- Cancel fault and display test functions shall be configurable to be accessed from level 1 or 2.
- All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.
- The control panel shall log a minimum of 700 events comprising of 100 event fire log and 200 event fault, disablement and historic logs, giving time, date, device reference and status of indication.
- Fire, fault and disablement events shall be logged as they occur. Visual and audible conformation shall be given on an array of LEDs, the Liquid Crystal Display and the internal supervisory buzzer.
- The control panel shall have an integral automatic power supply and maintenance free sealed battery, providing a standby capacity of a minimum 72 hours and further 30 minutes under full alarm load conditions. The system shall be capable of full re-charge within 24 hours following full system discharge. The performance of the power supply and batteries shall be monitored and alarm rose, should a fault be detected. The system shall protect the batteries from deep discharge.
- All terminations within the control panel with the exception of the 230V mains connection will be via removable terminal screw fixing points.

- The control panel will have a programmable maintenance reminder to inform the user that maintenance of the system is required. This function shall provide the user with the option of a monthly, quarterly, annually or bi-annually reminder prompts. The maintenance reminder will be indicated on the control panel. This message shall be resettable by the user and will not require the intervention of specialist support. The control panel will provide programmable free text field as part of the maintenance reminder facility.
- The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.

Manual Controls

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Enter or modify device text label
- Setup maintenance reminder
- Assign or modify zones
- Disable zones, device, sounders, FRE contact, auxiliary contacts
- Enable zones, device, sounders, FRE contact, auxiliary contacts
- Action weekly test
- Disable loop

Cable entries – The control panel will include the necessary top entry and rear entry cable entry points.

Manual call points (MCP)

- MCP's shall be addressable and of the steady pressure break glass type manufactured to the requirements of BS 5839: Part 2. A test key shall be provided to allow the routine testing of the unit to meet the requirements of BS 5839 Part 1 1988, without the need for special tools or the need to unfasten the cover plate.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches. The device shall incorporate a short circuit isolation device and a red LED indicator.
- The MCP shall be suitable for surface or flush mounting. When flush mounted the device shall be capable of fixing to an industry standard single gang box.

Smoke detectors – Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

Heat Detectors

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved.
- The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.

Addressable detector bases

- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.

Audible Alarms – Electronic sounders shall be colored red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

Commissioning

- The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.
- The labeling of Device and Zone labels should be part of the system.
- Necessary Software to the control panel

11.2.27. Fire Suppression Systems

Portable Extinguishers (CO2 or Halon based Extinguishers are not acceptable) shall be placed at strategic stations.

11.2.28. High Sensitivity Smoke Detection System

General – The HSSD system shall provide an early warning of fire in its incipient stage, analyze the risk and provide alarm and actions appropriate to the risk. The system shall include, but not be limited to, a Display Control Panel, Detector Assembly and the properly designed sampling pipe network. The system component shall be supplied by the manufacturer or by its authorized distributor.

Regulatory Requirements

- National Electrical Code (NEC)
- Factory Mutual
- Local Authority having Jurisdiction

11.2.29. Access Control System

The Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on proximity as well as biometric technology for the critical areas and Proximity technology for non-critical areas. An access control system consisting of central PC, intelligent controllers, proximity readers, power supplies, proximity cards and all associated accessories is required to make a fully operational on line access control system. Access control shall be provided for doors. These doors shall be provided with electric locks, and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts.

The system should be designed and implemented to provide following functionality:

- Controlled Entries to defined access points
- Controlled exits from defined access points
- Controlled entries and exits for visitors
- Configurable system for user defined access policy for each access point
- Record, report and archive each and every activity (permission granted and / or rejected) for each access point.
- User defined reporting and log formats
- Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.

- Day, Date, Time and duration based access rights should be user configurable for each access point and for each user.
- One user can have different policy / access rights for different access points.

11.2.30. CCTV System

The critical area of the MDC along with the Non-critical area needs to be under constant video surveillance. The primary objective of implementing a CCTV system is to ensure effective surveillance of the area and also create a record for post event analysis. Monitoring cameras should be installed in proper areas to cover all the critical areas of the data centre. The scope of work involves supply, installation, commissioning, testing and maintenance of the Closed Circuit Television system for NOC room of OCAC. The CCTV system shall provide an on-line display of video images on monitor. The entire setup shall be monitored on 24/7 basis. Cameras with suitable lenses shall be used to view all the critical areas of the MDC & NOC.

The CCTV system shall be based on the use of fixed dome cameras. The system and each of its devices shall be designed to meet the site ambient temperature and the site environmental conditions and shall operate satisfactorily under the specified permitted voltage and frequency variation band of the power supply source system.
All outdoor cameras shall be IP 66 rated.

The CCTV System proposed to fulfill the overall surveillance / observation requirements and enhance the level of security necessary in a software establishment such as ours which shall be complete in all respects and shall comprise of following minimum items.

Capabilities:

- The system should provide clear & accurate indication of an intruder or abnormal movement within and around the Facility.
- The system shall provide visual images from the cameras located throughout the facility. The cameras located shall be fed into the Digital Video Server (DVS) located in the security room.
- The Digital Video Server shall consist of 16 channels Digital Multiplexer with built-in recording system into Hard Disk.
- The Main Security Control Room which shall house the Monitors and the Digital Video Management Server.
- The CCTV should be equipped with Digital recording facility for later scrutiny, with at least 30 days of recording facility.

11.2.31. Cameras:

- The cameras will be of 1/3" format CCD pickup device for fixed lens camera. The cameras are being used for special observation purposes and are being located both indoor and outdoor & mounted on specially designed suitable mounting arrangement for operation under all severe environmental conditions to which these will be subjected especially the outdoor locations.

The cameras being used at these locations shall have the following basic minimum requirements:

- The cameras shall be fixed dome cameras
- The cameras shall be complete with the latest state of the art optical systems, filters, light sensitive pickup systems suitable for capturing images with very low light levels, and necessary interlaced scanners, encoders, decoders, associated amplifiers, synchronization facilities and any interfacing adapters as required, with all systems of that type suitable for a compact, durable, distortion free and clear image processing type camera.
- The color cameras shall have a minimum resolution of 420 lines and sensitivity of 0.08 lux (colour) and 0.013 lux (monochrome).
- The preset accuracy for the camera shall be +/- 0.1degree maximum
- The camera shall resume after alarm to the previously programmed state of alarm after alarm acknowledgement.
- The cameras shall have automatic level control complete with auto iris, and gain control of the amplifier and shall be complete with spot filter as required.
- The cameras shall have automatic shutter or 100% closing iris to prevent burning-in of image pickup device when the camera is not in use, both the shutter and iris shall fully close upon failure of power supply in order to prevent damage.
- The cameras shall have standby circuitry for when the camera is not selected on any of the monitors. The beam current of the camera pickup device shall be switched off automatically.
- The cameras shall have automatic circuitry which relates the black level in the signal to the darkest spot of the picture (black level control), limits the video signal in case of scene high-lights in order to prevent overloading of the monitor (White limiter), and prevents the automatic sensitivity control from reacting to strong highlights (Peak white eliminator).
- The cameras shall have the features that shall prevent the occurrence of internal condensation or condensation on the window, necessary heaters/thermostats shall be provided as required.
- The cameras shall be provided with a local power distribution junction box, with local isolation switches and fuses to isolate each of the power circuits of the camera related to main camera power, and other circuits related to cooling fan, blower etc.

- The camera housing shall have a rain/sun shield and a weather protection feature with a minimum IP protection of IP66 for outdoor mounted cameras.
- For indoor cameras, the protection class shall be IP45
- The aperture ratio (f-number) of the lenses shall be selected such that, a good picture is obtained at night.
- Power supply units, as required for the cameras, shall be provided.

Each of the CCTV cameras shall be located, mounted, positioned and install such that:

- The camera and its supporting structures presence least obstruction of view and least obstruction for satisfactory movement and operation of the camera due to remote and local controls.
- The cameras shall not be mounted on vibrating structures, where this is not possible than special structures or other facilities/measures for reducing vibrations shall be provided.
- All the camera movements along with Pan and Tilt, and associated forces on structures are taken in to account during the design and installation of the cameras.
- The installation presence the least risk of accidental damage.
- The equipment and its components are accessible for maintenance.
- The vibration of any object shall be less than that specified for the camera

11.2.32. Monitors

- There shall be total of 2 Nos. of 21” monitors for each Digital Video Recorder one to view the multiplexed output & second to view the switched output. This monitor should be located in the main control room. The monitor shall be positioned such that room lights and windows are minimized.
- Each of the monitors used at the main control room and operator status shall have the following basic minimum requirements.
- The monitor shall be suitable for use as desktop units.
- The monitors shall be high-resolution video monitors. The monitor shall have a bandwidth of at least 10 MHz (-3dB) and a horizontal resolution in the center of the picture minimum 420 lines in the case of color monitor.
- The monitors shall have the facilities to loop the video signal through the other monitor.
- Each monitor shall have local control knobs and remote control equipment and panel for monitor controls associated with power on/off switch standby on/off switch and for adjustment brightness, contrast, horizontal hold, vertical hold etc.
- Monitor shall be suitable for use as desktop units or can be rack mounted with suitable racks as appropriate.

11.2.33. Video & Telemetry Cables

The video signal shall be transmitted using co-axial cable and control of all zoom lens and Pan-Tilt functions through twisted pair interconnected between receiver and DVR.

Cabling for CCTV shall cover:

- Video link
- Remote control of cameras in terms of its control of pan tilts zooms & focus.
- Power supply cables.

The cable shall be shielded or provided with facilities to avoid interference between signals.

The transmission losses shall be minimized and where required for satisfactory operation correction amplifiers are cable equalizes shall be provided in the monitors on the CCTV cabinets.

11.2.34. Cabinets

CCTV cabinets shall be provided near set of monitors. The cable from the camera shall be terminated in this cabinet from where these signals are distributed to the monitors.

All necessary video amplifiers, interfaces etc. that forms the part of the CCTV system shall be installed in the cabinet.

11.2.35. Dome Camera

The Dome camera unit shall be 1/3” CCD Color Dome camera and shall provide a minimum of 540 TV lines resolution. It shall have built-in 3 -9mm varifocal lens. The camera shall operate on minimum lux level not more than 0.15 lux .The complete unit shall be housed in an integrated dome and base unit, both preferably made from injection moulded plastic. It shall be possible to adjust the camera head inside the dome in both the planes so that it can be wall or ceiling mounted. The camera shall operate on 24 V AC or 12 volts D.C.

11.2.36. Digital Video Recorder (DVR)

The DVR shall provide a high quality recorder capable of storage and play back of images from at a rate of up to 400 Frames/ second (PAL) and shall posses an internal watchdog, duplex operation, Windows NT Operating system, watermarking of each frame, 8 alarm inputs, software configurable video motion detection and scheduled event recording.

The digital recorder shall comply or exceed the following design and performance specifications:

- The DVR Digital video recorder shall have 400 images/sec viewing speed as well as 40 images / sec recording speed

- The recorder shall have a minimum of 16 video inputs. It shall also have looping inputs for all 16 inputs
- The recorder shall run on Windows NT.
- The recorder shall provide PAL , the following recording resolutions shall be possible 320 x 288 / 640 x 288 / 640 x 576 / 352 x 288 / 704 x 288 / 704 x 576
- The DVR shall have 4 high speed USB ports
- The DVR shall be in a position to display 16 video images simultaneously on the DVR or the remote client from Multiple DVRS on the LAN.
- The recorder shall support instant playback and shall have programmable favorite channel selection.
- The recorder shall allow a minimum of 6 X digital zoom on playback
- The recorder shall support simultaneous playback and record full duplex operation.
- The recorder shall have the feature of an internal hardware watchdog. The reorder shall have an internal hard disc capacity of min 500 GB
- The DVR shall be of the same make as that of the cameras to ensure 100% system compatibility. All the components in the DVR including hard disc etc shall be provided for the manufactures factory not locally assembled DVRS shall be provided. 100 % finished goods shall be supplied from the manufacturer
- The DVR shall have each channel individually programmable.
- Remote workstation shall be in a position to administer / view live images / search and view playback images
- The recorder shall have 16 hard-wired alarm inputs, which shall be capable of configuring globally as normally open or normally closed. Each of these inputs shall be assigned to any or all of the cameras to trigger recording at custom record rates. Up to 5 seconds of pre-alarm shall also be available on each camera.
- The recorder shall provide 24 dry contact outputs, each of which shall be associated with any or all of the camera inputs and/or alarm inputs.
- The recorder shall provide an extremely flexible scheduling on a week-byweek basis. Each 24-hour period shall be divided into 15-minute blocks enabling different configurations of recording triggers to be available during each 15-minute period.
- The recorder shall provide onscreen controls for operation of PTZ cameras. All fully functional cameras shall be controlled via a PC comport which shall use an additional converter to communicate via RS485/422
- The recorder shall provide an Ethernet port as standard. If required in addition free client software shall supplied which enables remote control and connectivity via TCP/IP. The DVR shall support Gigabit port 10/100/1000 base T

- The recorder shall be tested to comply with UL regulations/certifications.
- The recorder shall provide a screen resolution of 1280 x1024 (XVGA output)
- The recorder shall have a built in watchdog that will automatically restart after a power failure and begins to record as per its configured settings.
- The recorder shall provide the ability to manually 'back up' recorded data to hard disk or DVD / RAID while the unit continues to record.
- The recorder shall be programmed using a keyboard and mouse via on screen menus.
- The recording of the recorders are watermarked and encrypted requiring backup software to open and view them. In addition, images backed up in bitmap or JPEG format can be verified for authenticity
- The recorder shall be suitable for mounting on a standard 19" rack.
- There shall be a network management Digital Video Recorder (DVR) if more than DVR is required to allow viewing of cameras from multiple DVR's in any combination.
- The DVR shall support pre-alarm and post alarm recording.
- The DVR shall support CIF / 2CIF and 4 CIF resolutions while recording

11.2.37. Building Management System (BMS) for OSWAN NOC, helpdesk room and UPS room.

The building management system shall be implemented for effective management, monitoring and Integration of various components like HVAC systems, Access Control systems, fire detection system etc.
The BMS shall perform the following general functions including but not limited to:

- Building Management & Control
- Data Collection & archival
- Alarm Event & Management
- Trending
- Reports & MIS Generation
- Maintenance & Complaint Management

The scope of work shall include designing supplying and installing of Building management (Automation) System. The work shall consist of furnishing all materials, equipment's and appliances necessary to install the said system, complete with Sensors, Direct Digital Controllers, Communication Controllers and Supervisory Software complete with necessary software/hardware support for interfacing with other systems. It shall include laying of cabling duct, conduits and power supply etc., necessary for installation of the system with supply of appropriate type products. The controller shall be 32/64 bit based Microprocessor Controller and shall sit directly on the TCP / IP

network. The controller shall be Web Based, Web Enabled, Real Time Clock, and Web Browser with Communication speed min of 10/100 Mbps.

Agency shall design & provide a full Building automation system on the basis of truly distributed intelligence and shall comprise of the following general functional sub systems.

- Air Conditioning Management & Control
  - Precision AC Units
- Temperature monitoring and controls at all specified positions/locations
- Energy Management
  - LT Panel Energy Monitoring
  - UPS Monitoring
- Safety & Security Systems Integration
  - Fire Alarm System Integration
  - Access Control & Surveillance System Integration
  - Gas System Integration
- Integration
  - DG Set on MODBUS Protocol with RS 485 Communication Port
  - Energy Meter on MODBUS Protocol with RS 485 Communication Port

11.2.38. Water Leak Detection System

The water leak detector shall be installed to detect any seepage of water into the critical area and alert the Security Control Room for such leakage. It shall consist of water leak detection cable and an alarm module. The cable shall be installed in the ceiling & floor areas around the periphery.

- Water Leak Detection system should be for the Server and Network room areas to detect and water flooding below the floor.
- Water Leak Detection System should be wire based solution with alarm; the wire needs to lay in MDC area surrounding the PAC units & NOC area as well, which is the probable source of water leakage.

11.2.39. Fire Proof Enclosures for Media Storage

The overall design of the safe should be suitable for safe storage of computer diskettes, tapes, smart cards and similar devices and other magnetic media, paper documents, etc. the safe should have adequate fire protection.

Capacity	**150 Litres**
Temperature to Withstand	1000° C for at least 1 hour
Internal Temperature	30° C after exposure to high temperature for 1 hour
Locking	2 IO-lever high security cylindrical / Electronic lock

11.2.40. Public Address System

The PA system is required for: (Optional)

- Making public announcement from the Security Control Room and Facility Manager's room. Clear and crisp announcement should reach to the entire Facility area.
- Microphones should be provided to make announcements / respond to announcement from the designated location within the Facility.
- To play light music if required.

11.2.41. Common Alarm System

- The common alarm panel is required for checking the healthiness of all systems, to be installed at Server Firm Area & NOC Area
- The panel can be installed in suitable location at OCAC.
- The common alarm panel should have provision for accepting "potential free" signals from all system for relevant status change in that system

11.2.42. Electrical Panels

- The Panels shall be of compartmentalized design so that circuit arc / flash products do not create secondary faults and be fabricated out of high quality CRCA sheet, suitable for indoor installation having dead front operated and floor mounting type.
- All CRCA sheet steel used in the construction of Panels shall be 2 mm. thick and shall be folded and braced as necessary to provide a rigid support for all components. Joints of any kind in sheet steel shall be seam welded, all welding slag grounded off and welding pits wiped smooth with plumber metal.
- The Panels shall be totally enclosed, completely dust and vermin proof and degree of protection being not less than IP: 54 to IS: 2147. Gaskets between all adjacent units and beneath all covers shall be provided to render the joints dust proof. All doors and covers shall be fully gasketed with foam rubber and /or rubber strips and shall be lockable.
- All panels and covers shall be properly fitted and secured with the frame and holds in the panel correctly positioned. Fixing screws shall enter into holes, taped into an adequate thickness of metal or provided with bolts and nuts. Self-threading screws shall not be used in the construction of Panels.
- A base channel of 75 mm. x 50 mm. x 6 mm. thick shall be provided at the bottom.
- Panels shall be preferably arranged in multi-tier formation. The size of the Panels shall be designed in such a way that the internal space is sufficient for hot air movement. If necessary, openings shall be provided

for natural ventilation, but the said openings shall be screened with fine weld mesh. The entire electrical component shall be derated for 50°c.

- The Panels shall be provided with removable sheet steel plates at top and bottom to drill holes for cable / conduit entry at site.
- The Panels shall be designed to facilitate easy inspection, maintenance and repair.
- The Panels shall be sufficiently rigid to support the equipment without distortion under normal and under short circuit condition. They shall be suitably braced for short circuit duty

11.2.43. Circuit Compartments

- Each MCCB shall be housed in separate compartments and shall be enclosed on all sides. Sheet steel hinged lockable door shall be duty interlocked with the unit in `ON' and `OFF' position.
- All instruments and indicating lamp shall be mounted on the compartment door. Sheet steel barriers shall be provided between the tiers in a vertical section.

11.2.44. Instrument Compartments

- Separate adequate compartments shall be provided for accommodating instruments, indicating lamps, control contactors/ relays and control fuses etc.
- These components shall be accessible for testing and maintenance without any danger of accidental contact with live parts, bus bar and connections

11.2.45. Bus-bars

- The busbar shall be air insulated and made of high quality, high conductivity, high strength Aluminium.
- The busbar shall be of 3 phases and neutral system with separate neutral and earth bar. The size of neutral busbar in all main panels or lighting panels and feeders for panel shall be equal to phase busbar.
- The busbar and interconnection between busbars and various components shall be of high conductivity Aluminium.
- The busbar shall be of rectangular cross-section designed to withstand full load current for phase busbars and half rated current for neutral busbars in case of MCC panels only and shall be extensible on either side.
- The busbar size shall be as per the rating of the panel. The busbar shall have uniform cross-section throughout the length.

- The busbars and interconnections shall be insulated with epoxy-coated busbar. The busbar shall be supported on bus insulators of non flammable type with high creepage and high anti tracking property and non-hydroscopic SMC / DMC insulated supports at sufficiently close intervals to prevent busbars sag and shall effectively withstand electromagnetic stresses in the event of short circuit.
- The busbar shall be housed in a separate compartment. The busbar shall be isolated with 3-mm. thick bakelite sheet to avoid any accidental contact. The busbar shall be arranged such that minimum clearance between the busbar are maintained as below:
  - Between phases: 25 mm. minimum
  - Between phases and neutral: 25 mm.
  - Between phases and earth: 25 mm.
  - Between neutral and earth : 20 mm. minimum
- All busbar connections shall be done by drilling holes in busbars and connecting by chromium plated or tinned plated brass bolts and nuts.
- Additional cross-section of busbar shall be provided in all Panels to cover up the holes drilled in the busbar. Spring and flat washers shall be used for tightening the bolts.
- All connections between busbars and circuit breakers / switches and cable terminals shall be through aluminum strips of proper size to carry full rated current. These strips shall be insulated with insulating taps.
- Panel to panel entry of bus bar shall be effectively sealed by electrical and thermal insulation barriers so that products of flashover do not travel from one panel to another panel creating multiple faults.
- Busbar calculated on 50 deg. C. ambient temp. and 85 deg. C. for continuous and short time rating. Busbar surrounded air temp. shall be considered 70deg. C. for busbar calculation
- All joint shall have non-flammable insulation shrouds for secondary insulation purpose

11.2.46. Electrical Power and Control Wiring Connection

- Terminal for both incoming and outgoing cable connections shall be suitable for 1100 V grade, aluminium / copper conductor XLPE insulated and PVC sheathed, armored cable and shall be suitable for connections of solder less sockets for the cable size as per the feeder capacity.
- Power connections for incoming feeders of the main Panels shall be suitable for 1100 V grade aluminium conductor (XLPE) cables.
- Both control and power wiring shall be brought out in cable alley for ease of external connections, operation and maintenance.
- Both control and power terminals shall be properly shrouded.

- 10% spare terminals shall be provided on each terminal block. Sufficient terminals shall be provided on each terminal block, so that not more than one outgoing wire is connected to per terminal.
- Terminal strips for power and control shall preferably be separated from each other by suitable barriers of enclosures.
- Wiring inside the modules for power, control, protection and instruments etc. shall be done with use of 660 / 1100 V grade, FRLS insulated copper conductor cables conforming to IS standards. For current transformer circuits, 2.5 sq.mm. copper conductor wire shall be used.
- Other control wiring shall be done with 1.5 sq.mm. copper conductor wires.
- Wires for connections to the door shall be flexible. All conductors shall be crimped with solder less sockets at the ends before connections are made to the terminals.
- Control power supply to modules through the control transformer Control power wiring shall have control fuses, (HRC fuse type) for circuit protection. All indicating lamps shall be protected by HRC fuses.
- Particular care shall be taken to ensure that the layout of wiring is neat and orderly. Identification ferrules shall be filled to all the wire termination for ease of identification and to facilitate checking and testing

11.2.47. Terminals

- The outgoing terminals and neutral link shall be brought out to a cable alley suitably located and accessible from the panel front.
- The current transformers for instruments metering shall be mounted on the disconnecting type terminal blocks.
- No direct connection of incoming or outgoing cables to internal components of the distribution board is permitted; only one conductor may be connected in one terminal

11.2.48. Cable Compartments

- Cable compartments of minimum 300 mm size shall be provided in the Panels for easy termination of all incoming and outgoing cables entering from bottom or top.
- Adequate supports shall be provided in the cable compartments to support cables.
- All outgoing and incoming feeder terminals shall be brought out to terminals blocks in the cable compartment.

11.2.49. Labels

- Engraved PVC labels shall be provided on all incoming and outgoing feeders.
- Single line circuit diagram showing the arrangements of circuit inside the distribution board shall be pasted on inside of the panel door and covered with transparent laminated plastic sheet.

11.2.50. Name Plates

- A nameplate with the Panels designation in bold letters shall be fixed at top of the central panel.
- A separate nameplate giving feeder details shall be provided.
- Inside the feeder compartments, the electrical components, equipments, accessories like switchgear, control gear, lamps, relays etc. shall suitably be identified by providing stickers.
- Engraved nameplates shall preferably be of 3 ply, (Red-White-Red or Black- White-Black) lamicold sheet. However, black engraved perplex sheet name plates shall also be acceptable. Engraving shall be done with square groove cutters.
- Nameplate shall be fastened by counter sunk screws and not by adhesives

11.2.51. Danger Notice Plates

- The danger notice plate shall be affixed in a permanent manner on operating side of the Panels.
- The danger notice plate shall indicate danger notice in English, Hindi and Odiya and with a sign of skull and bones.
- The danger notice plates, in general, meet the requirements of local inspecting authorities.
- Overall dimensions of the danger notice plate shall be 200 mm. wide x 150 mm. high.
- The danger notice plate shall be made from minimum 1.6 mm. thick mild steel sheet and after due pre-treatment to the plate, the same shall be painted white with vitreous enamel paint on both front and rear surface of the plate.
- The letters, figures, conventional skull and bones etc. shall be positioned on plate as per recommendation of IS: 2551-1982.
- The said letters, the figures and the sign of skull and bones shall be painted in signal red colour as per IS: 5-1978.
- The danger plate shall have rounded corners. Location of fixing holes for the plate shall be decided to suit design of the Panels.

- The danger notice plate, if possible, it should be of ISI certification mark

11.2.52. MCCB

- The moulded case circuit breaker (MCCB) shall be air break type and having quick make - quick break with trip free operating mechanism.
- Housing of the MCCB shall be of heat resistant and flame retardant insulating material.
- Operating handle of the MCCB shall be in front and clearly indicate ON/OFF/TRIP positions.
- The electrical contact of the circuit breaker shall be of high conducting non deteriorating silver alloy contacts.
- The MCCB shall be provided microprocessor based overload and short circuit protection device.
- All the releases shall operate on common trip busbar so that in case of operation of any one of the releases in any of the three phases, it will cut off all the three phases and thereby single phasing of the system is avoided.
- The MCCB shall provide two sets of extra auxiliary contacts with connections for additional controls at future date.

11.2.53. Contactors

- The contactors shall meet with the requirements of IS: 2959 and BS: 7755.
- The contactors shall have minimum making and breaking capacity in accordance with utilization category AC3 and shall be suitable for minimum Class II intermittent duty.
- If the contactor forms part of a distribution board then a separate enclosure is not required, but the installation of the contactor shall be such that it is not possible to make an accidental contact with live parts

11.2.54. Indicating Lamps

- Indicating lamps assembly shall be screw type with built in resistor having non-fading colour lens. LED type lamps are required.
- Wiring for Remote ON, OFF, TRIP indicating lamp is required.
- Colour shade for the indicating lamps shall be as below :
  - ON indicating lamp : Red
  - OFF indicating lamp : Green
  - TRIP indicating lamp : Amber
  - PHASE indicating lamp : Red, Yellow, Blue
  - TRIP circuit healthy lamp : Milky

11.2.55. Cable Trays

The cable trays shall be of ladder type / perforated steel section slotted angles. The trays shall be complete with plates, Ts, elbows, risers, and all necessary hardware. The trays shall be galvanized as per IS 2629. The cable trays shall have suitable strength and rigidity to provide adequate support for all cables. It shall not present sharp edges, burs of projections, injurious to the insulation of the wiring and cables. The trays shall be adequately protected against corrosion and shall be made of corrosion resistant material. It shall have side rails or equivalent structural members. There shall be a continuous earth strip running on either side of the tray for earthing. The distance between power cable tray/ conduit and data cable tray/ conduit should be between 1 to 1.5 feet.

11.2.56. Earthing

Sl. No	Requirement	Compliance (Y/N)	Remark (If any)
1	The earthing pit should be a borehole of at least 500 mm diameter and 3.5 meters deep		
2	Pipe electrode made of a 65 mm diameter GI perforated pipe of 3.0-meter length attached at the top with a funnel covered with wire mesh.		
3	Annular space between the electrode and borehole walls with layers of chemical compounds.		
4	G.I. strip fixed to the electrode to act as an earthing connection		
5	100 mm of the chamber above ground level		
6	laying of earth wires or GI/copper strips between the earth electrode and the electrical room		
7	The Earth pit shall conform in all respects to IS: 3043-1987 standard with latest amendments		
8	Ground resistance should be less than 1 ohm, not to exceed 5 ohm		
9	Earth pit covers shall be made of high-quality PVC or high-grade cast iron.		
10	Earth pit covers should be rust free & Earth pit should be maintenance free.		

11.2.57. Video Wall (3x2) with Controller

Sl.No	Requirement		Compliance (Y/N)	Remark (If any)
1	Display Wall Screen Configuration	3x2		
2	Total No. of Displays	6		

3	Display Screen Size	55” (diagonal)		
4	Panel Technology	IPS		
5	Brightness	700nit		
6	Response Time	8ms		
7	Viewing Angle	178/178		
8	Resolution	1920 x 1080		
9	Contrast Ratio	1000:1		
10	**Input Connectivity**			
i	Digital	HDMI(1), DVI-D(1) or DP (1)		
ii	Analog	RGB(1)		
11	Audio	Shall support external Audio inputs		
12	External Control	RS232C (In/Out), RJ45		
13	Sensor	IR, Ambient		
	Output Connectivity			
14	Digital	RGB: DP1.2 (Loop-out)		
15	Bezel to Bezel Gap	0.88mm		
16	Video Controller	Should be from same or different OEM as video wall		
i	Video Input Interfaces	8 x HDMI Type A Female (Black)		
ii	Video Output Interfaces	8 x HDMI Type A Female (Black)		
Iii	Should support real-time switching stable signal transmissions.			
Iv	Should allow user to create custom video wall layouts via intuitive web GUI			
v	Should support video scaling function to convert input resolutions to the optimum display resolutions			
Vi	Should support system management via front-panel push buttons, IR, RS-232 and Ethernet (Telnet / Web GUI) connections			
Vii	Supports IR signals for remote control			
Viii	Rack Mountable (1U design)			

11.2.58. CAT 6A U/UTP LSZH Cable

Sl.No	Requirement	Compliance (Y/N)	Remark (If any)
1	CAT6A U/UTP 23 AWG Cable should meet and exceed ANSI/TIA 568.2-D Category 6A and ISO/IEC 11801 Class EA Specifications		
2	Cable shall be constructed with pair separator as well		

	as individual conductor separator.		
3	The cable shall have special jacket design to mitigate A-NEXT challenges in CAT6A UTP channel. The nominal Outside diameter should be 7.1 – 7.3 mm		
4	**Electrical properties:**		
	Max DC Resistance: ≤7.61 Ohms/100m		
	Max. Operating voltage: 80 V		
	Frequency: up to 550 Mhz		
	Mutual Capacitance: 6.0 nF/100m @1kHz		
5	**Environmental & Safety features:**		
	Operating temperature of -20 to 60 ^{0}C		
	The cable shall have Low-Smoke, Zero Halogen (LSZH) jacketing and must comply with the following Fire Safety standards: 1) ISO/IEC 60332-3-22: Vertical Flame Spread 2) ISO/IEC 60754-2: Acidity 3) ISO/IEC 61034-2: Smoke Density		
	Cable shall be compliant to the Fire performance as per EN50575 standard and meet CPR rating of Dca, at a minimum.		
6	**Certifications and Test Reports:**		
	Category 6A cable along with offered channel components should be certified by Intertek lab under 4 connector channel configuration to the requirement of ANSI/TIA 568-C.2 for long channel (100m) as well as short links (<15m). Test Certificates to be provided with bid.		
	Cable shall be ETL verified as per ANSI/TIA 568-C.2 and ISO/IEC 11801 for CAT6A requirements.		
	CAT6A Cable must support IEEE 802.3bt Type 4 requirements for remote powering (4PPoE).		
	Factory test reports for CAT6A cable must be available for verification of authenticity, at OEM website with unique print string on individual cable jacket.		

11.2.59. Category 6A U/UTP Modular Information Outlets

Sl. No	Requirement	Compliance (Y/N)	Remark (If any)

1	The CAT6A UTP 8-pin modular (RJ-45) jacks shall have Electrical performance guaranteed to meet or exceed the channel specifications of ISO/IEC 11801 Class EA and ANSI/TIA-568-C.2 Category 6A.		
2	Shall support network line speeds up to at least 10 gigabits per second		
3	Each outlet shall be supplied with rear protective strain relief cap to protect against contamination and securing the termination.		
4	**Electrical properties:**		
4.1	The information outlet shall have a Current Rating of 1.5 A at 20°C		
4.2	Insulation Resistance, minimum: 500 MOhm		
4.3	Contact Resistance, maximum: 100 mOhm		
4.4	Contact Resistance Variation, maximum: 20 mOhm		
5	**Mechanical performance:**		
5.1	Material: High-impact, flame retardant, thermoplastic, UL 94V-0 rated		
5.2	Shall be IEC 60603-7 certified.		
5.3	Plug insertion life, Min: 750 cycles		
5.4	Plug retention force, min: 130N		
5.5	Should be UL and cUL listed		
6	**Single Port Faceplate:**		
6.1	Faceplate shall be available in 1 or 2 port square version, with dust caps or shutter.		
6.2	Faceplate Material shall be high impact, flame retardant, UL-rated 94 V-0, thermoplastic.		

11.2.60. Category 6A U/UTP Patch Cord

Sl.No	Requirement	Compliance (Y/N)	Remark (If any)
1.	CAT6A U/UTP Patch Cord, shall be of 4 pair solid construction, with pair separator.		
2.	Offered CAT6A Patch cord shall support intelligent cable detection mechanism and function when used with AIM system.		
3.	Plugs shall be designed with an anti-snag latch to facilitate easy removal during move, add and change processes.		
4.	The cordage shall be UTP components that do not include internal or external shields, screened		

	components or drain wires.		
5.	Patch Cord shall have LSZH jacket complying with the following Fire Safety standards: ISO/IEC 60332-3-22: Vertical Flame Spread ISO/IEC 60754-2: Acidity ISO/IEC 61034-2: Smoke Density		
6.	Patch Cord shall have min plug insertion life of 750 cycles.		
7.	Min Plug retention force: 130N		
8.	Shall be ETL certified.		
9.	Patch Cords shall have maximum dc Resistance:0.30 Ohm		

11.2.61. Category 6A U/UTP Patch Panel

Sl.No	Requirement	Compliance (Y/N)	Remark (If any)
1.	Patch Panel shall be CAT6A UTP 24 port, loaded 1U compliant to ANSI TIA 568-C.2		
2.	The patch panel shall be available in 1U (24 port) or 2U (48 port) panel capable of supporting 24 or 48 unshielded modular 8-pin connectors certified for IEC 60603-7-4 while meeting the CAT6A Channel Performance.		
3.	The panel shall be equipped with rear cable management with min 4 nos of cable bundle managers for 24 port, and 8 nos of bundle managers for 48 port panel.		
4.	The panel must be capable of supporting an upgrade to intelligent system without any interruption to service due to patch cord removal or terminal block re-termination.		
5.	Panel shall have plug retention force of 130N min.		
6.	The panel shall be UL Listed		
7.	**Electrical performance:**		
7.1	Current Rating - 1.5 A @ 20 °C Dielectric Withstand Voltage, RMS - 1500 Vac @ 60 Hz Insulation Resistance, minimum - 500 MOhm		
8	Operating temperature: -10 °C to +60 °C		
9	Insertion Life = 750 minimum insertions		
10	Panel must be certified for CAT6A transmission by Intertek under 4 connector channel configuration.		

11.2.62. MPO – LC 24F Cassette (2x12MPO)

Sl.No	Requirement	Compliance (Y/N)	Remark (If any)
1.	MPO - LC Modules – 12-fiber or 24-fiber – Shall be available in 50 micron lazer optimized OM4 or the latest OM5 versions.		
2.	The 24-fiber module shall have 12 pre-installed duplex LC adapters at the front routed to 2 pre-installed 12-fiber Low loss MPO adapters at the back.		
3.	All MPO modules must support 'Method B' wiring pattern for ease of scalability. Same cassette should be used in both end of the link, without need of flipped or straight wiring management.		
4.	Dust caps on each front port must be translucent to support VFL tests, without removing caps. Test light should be visible at the remote end, even with dust caps ON.		
5.	The cassettes shall be cUL US 1863 listed. Max Insertion Loss (MPO): <0.35dB.		
6.	MPO Modules must be Intelligent ready and support upgrade to full intelligent system with 'zero downtime', i.e. without removing any patched connection or changing any installed hardware.		
7.	The offered MPO cassettes must meet the applications length limits as specified above in the RFP.		
8.	Factory Test report: Shall be available pub **MPO – LC 24F Cassette (2x12MPO)** likely against unique tracking ID on MPO Module, at OEM website.		

11.2.63. HIGH DENSITY 1U MODULAR FIBER PANEL

Sl.No	Requirement	Compliance (Y/N)	Remark (If any)
1.	Capacity & Type: High Density 1U sliding fibre panel enclosure, accepts (4) MPO modules, for up to 48 duplex LC (96 fibre) termination High Density 2U sliding fibre panel enclosure, accepts (12) MPO modules, providing min 144 duplex LC ports (288 fibres)		

2.	The 1U / 2U shelves shall be equipped with a front trough and door for patch cord management and port labelling.		
3.	Fiber shelf shall have front sliding mechanism with positive locking, for increases access.		
4.	High Density Fiber Shelves shall have the feature to pull out half of the tray to facilitate easy access during installation and service, without disturbing the other half in the same tray. This is an essential feature to ensure safe access in high density shelf.		
5.	All Fiber shelves shall support both rear and side entry for trunk cables for better routing and access. Shall be made of powder coated steel with min 21 inch depth for storage of fibre trunks.		
6.	The panel and shelves shall support upgradable to Intelligent system without any network downtime, or removal of patched connections.		
7.	UL 94 V-0 rated material.		

11.2.64. 12F MPO TRUNK CABLE, OM4

Sl.No	Requirement	Compliance (Y/N)	Remark (If any)
1.	Low Loss MPO-12/UPC to MPO-12/UPC, Pre-terminated, LSZH, Bend Insensitive OM4 Trunk Cable		
2.	All cables shall be constructed with one or more subunits, each with 12 fibres surrounded by a jacket containing aramid yarn strength members.		
3.	All cables should be Bend insensitive multimode OM4 or OM5.		
4.	Cable shall comply to the standard requirements for ANSI/ICEA S-83-596, Telcordia GR-409, IEC 60794-1, IEC 60793-2-10, type A1a.3a, IEC 60793-2-10, type A1a.3b and TIA-492AAAD (OM4)		
5.	Flame rating shall be NEC OFNR-LS (ETL) The cable must have the flame test compliance to IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE 383, UL 1666 and UL 1685		
6.	The Trunk cable shall have Method B construction		
7.	Cable MPO connector shall have Max Insertion Loss of 0.20dB		

	Min Return loss of MPO shall be ≥ 27dB.		
8.	Cable shall have OD of 5.2 – 5.8mm. Tensile strength shall be up to 650N.		
9.	All OM4 trunk cables must have Aqua coloured jacket as per TIA and ISO standards recommendation.		
10.	Cable must be EN50575 CPR Cable Euro Class certified as per Dca.		
11.	The offered MPO cable must meet the applications length limits as specified above in the RFP.		

11.2.65. LC – LC Multimode Duplex Fiber Patch Cords, LSZH

Sl.No	Requirement	Compliance (Y/N)	Remark (If any)
1.	LC/UPC to LC/UPC, Multimode OM4 duplex Patch Cord, bend insensitive Fiber 1.6mm Duplex patch cords.		
2.	Low Smoke Zero Halogen (LSZH) compliant to IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE 383, UL 1666, UL 1685		
3.	Flame Test Listing: NEC OFNR-LS (ETL)		
4.	Patch Cord shall support intelligent sensing of connections in each port when used with an AIM system.		
5.	Connector Optical Performance Insertion Loss, max.: 0.20 dB Return Loss, minimum: 35.0 dB		
6.	Cord shall be EN 50575 CPR rated.		
7.	OM4 Patch Cord Jacket colour: Aqua.		

11.2.66. SC – LC Singlemode Duplex Fiber Patch Cords 15 Mtr, LSZH

Sl.No	Requirement	Compliance (Y/N)	Remark (If any)
8.	SC/UPC to LC/UPC, Singlemode OM4 duplex Patch Cord, bend insensitive Fiber 1.6mm Duplex patch cords.		
9.	Low Smoke Zero Halogen (LSZH) compliant to IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE 383, UL 1666, UL 1685		
10.	Flame Test Listing: NEC OFNR-LS (ETL)		
11.	Patch Cord shall support intelligent sensing of connections in each port when used with an AIM		

	system.		
12.	Connector Optical Performance Insertion Loss, max.: 0.20 dB Return Loss, minimum: 35.0 dB		
13.	Cord shall be EN 50575 CPR rated.		
14.	OM4 Patch Cord Jacket colour: Aqua.		

11.2.67. IP KVM Switch

Sl.No	Requirement	Compliance (Y/N)	Remark (If any)
1.	Enclosure Type : Rack mountable		
2.	Ports: 24 x KVM Ports, IP KVM Local User: Minimum 1 local user.		
3.	Resolution: 1600 x 1200 @ 60 Hz		
4.	Key Board & Mouse Interface: PS2, USB		
5.	Authentication Method: Active Directory, LDAP, RADIUS		
6.	Interface: Ethernet 10 Base-T/100 Base-TX/1000 Base-T, Quantity: Minimum 24, Connector Type: 18 pin SPHD, RJ45		
7.	Encryption Algorithm: 128 bit AES, DES, RSA, SSL		
8.	Remote Management Protocol: HTTP		
9.	Status Indicators: Minimum Port and power status		
10.	Features: Onscreen Display, Firmware upgradable and manageable		
11.	Compatibility: Mac, PC, Un ix/Linux		
12.	Accessories: Rack mount kit, Power cable & serial adapters to be included		
13.	Warranty: Comprehensive onsite: 5 Years		

11.3. IT Infrastructure Technical Specifications:

11.3.1. DMZ Switch

Make: **Model:**			
Sl#	**Requirement**	**Compliance (Y/N)**	**Remark (If any)**
	General Requirement		
1	Data centre class Layer-3 switch with 48 Fiber downlink ports capable of supporting 10Gbps		

Make: **Model:**			
Sl#	**Requirement**	**Compliance (Y/N)**	**Remark (If any)**
	Ethernet or 32Gbps Fiber Channel and 6 x 40/100G QSPF28 uplink ports from Day 1.		
2	The Switch should be activated with 24 downlink and 6 uplink ports from Day 1 and have option of license base activation of remaining 24 downlink ports for future use		
3	Proposed Switch must be 19'' rack mountable		
4	Network Infrastructure equipment must use 240V AC power.		
5	The switch should have redundant Power supply and Fan supporting to control the switch temperature.		
	Hardware and Interface Requirement		
6	Switch should have the following interfaces:		
	Switch should have 48 x 10GBaseT ports and 6 x 40/100G fixed ports		
7	Switch should be populated with multi core CPU		
8	The switch should support minimum 24 GB System memory		
9	The switch should support above 64 GB Flash/SSD		
10	The switch should support minimum 32 MB Buffer memory		
11	Switch should have console port for local management & management interface for Out of band management		
	Performance Requirement		
12	Switch should support 3 Tbps of bandwidth with 1200 Mpps of Forwarding rate		
13	Switch should support 200K MAC Addresses entries		
14	Switch should support minimum 64 Equal-cost multipath		
15	Switch should support minimum 1600000 LPM routes		
16	Switch should support minimum 2000 VRF instances		
	Network Virtualization Features		
17	Switch should support Software Defined Networking Solution		
18	Switch should support standards based VXLAN EVPN fabrics		

Make: **Model:**			
Sl#	**Requirement**	**Compliance (Y/N)**	**Remark (If any)**
	Layer2 Features		
19	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)		
20	Switch should support VLAN Trunking (802.1q)		
21	Switch should support Port-Channel across multiple switches		
22	Switch should support Port-Channel across multiple switches		
23	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy		
	Layer3 Features		
24	Switch should support static and dynamic routing (OSPF, BGP)		
25	Switch should support segment routing and VRF route leaking functionality from day 1		
26	Switch should provide multicast traffic reachable using: a. PIM-SM (RFC 4601) b. PIM-SSM (RFC 3569) c. Support Multicast Source Discovery Protocol (MSDP) (RFC 3618)		
	Quality of Service		
27	Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point)		
28	Switch should support for different type of QoS features for ream time traffic differential treatment using a. Weighted Random Early Detection b. Strict Priority Queuing		
29	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
	Security		
30	Switch should support for external database for AAA using:		

Make: **Model:**			
Sl#	**Requirement**	**Compliance (Y/N)**	**Remark (If any)**
	a. TACACS+ b. RADIUS		
31	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding		
32	Switch platform should support MACSec (802.1AE) in hardware		
33	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined		
	Manageability		
34	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail		
35	Switch should provide remote login for administration using: a. Telnet c. SSHv2		
36	Switch should support for management and monitoring status using different type of Industry standard NMS using SNMP v3 with Encryption		
37	Switch should provide different privilege for login in to the system for monitoring and management		
	Certification:		
38	The switch should have CE Marking and ROHS-6 compliant		
39	The switch should have UL 60950-1, EN 60950-1 Second Edition, safety standard compliance and EN55022 Class A, ICES003 Class A, VCCI Class A, EN61000-3-3 EMC compliance		
40	**Gartner:**		
	Switch OEM must be in ‘leaders’ or 'Challengers' in the Gartner Magic Quadrant for wired & wireless networking latest published by Gartner.		
	Warranty:		
41	Comprehensive Onsite OEM Warranty for 5 Years		

11.3.2. 24 port L3 Network Switch

Make: **Model:**			
Sl. No.	**Specification**	**Compliance (Yes/No)**	**Deviation (If Any)**
1.	Switch should be 1 RU with minimum 24 no. of 1/10G SFP + ports loaded with 24 numbers of 10G SFP+ single mode transceivers from Day One.		
2.	Switch should have minimum 320 Gbps of stacking bandwidth with dedicated stacking ports and cables with minimum 4 switches in a single stack.		
3.	Switching system shall have minimum 480 Gbps of switching fabric and minimum 450 Mpps of forwarding rate.		
4.	Switch should have hot swappable 1:1 redundant power supply.		
5.	Power supply, fan modules and interface modules should be hot swappable.		
6.	Switching system shall have minimum 32K MAC Addresses and 1K active VLANs.		
7.	Switch should support minimum 2K ACLs, 4K Multicast and 24K Routes.		
8.	Should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.1AS, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.		
9.	Should have static routing, OSPF, OSPFv3, BGP, HSRP for IPv6/VRRPv3, VRF (Virtual routing and forwarding), IGMP v1/v2/v3, PIM and multicast routing.		
10.	Shall have 802.1p class of service, marking, classification, policing and shaping. Should support strict priority queuing.		
11.	Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+		
12.	Switch should support port security, DHCP snooping, Dynamic ARP inspection, IP Source guard, BPDU Guard, Spanning tree root guard.		
13.	Switch should support IPv6 Snooping, IPv6 RA Guard, IPv6 First Hop Security, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.		
14.	Should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment.		
15.	Should support 2000 or more aggregate policers or QoS ACLs per switch		
16.	Switch should support traffic monitoring based on sflow/jflow/netFlow technology.		
17.	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.		
18.	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.		
19.	Switch / Switch's Operating System should be tested and certifiedfor EAL 2/NDPP or above under Common Criteria Certification.		
20.	Switch shoudl be IPv6 Certified/IPv6 logo ready.		
21.	The product must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for wired and wireless LAN Access Infrastructure published by Gartner.		
22.	OEM should be ISO 9001:2008 or latest and 14001:2004 Certified.		
23.	Comprehensive OEM Warranty for 5 Years		

11.3.3. Access (PoE) Switch

Make: **Model:**			
Sl#	**Requirement**	**Compliance (Y/N)**	**Remark (If any)**
1	Switch architecture should be Fixed Form factor/ stackable based		
2	Switch should have wire-speed, non-blocking and distributed forwarding on all the ports		
3	Switch should have minimum of 24 x 10/100/1000 Mbps RJ45 plus 2 x 1/10G SFP+ uplink ports with 2 Nos. 10G SFP+ (SM) Trans receiver module from day-1.		
4	Switch should have minimum stacking bandwidth of 40 Gbps or more (In addition to above asked ports and bandwidth) and stacking up to 4 units in a single stack from day-1.		
5	Switch should have wire speed of data switching capacity and forwarding throughput (Mpps)		
6	Switch should support min 32K MAC addresses and min 2000 active VLANs and 10MB packet buffer.		
7	Switch should have full Layer 2 features and support spanning tree protocols standards like STP (IEEE 802.1d), MSTP(IEEE 802.1s) RSTP (IEEE 802.1w) etc. LACP/IEEE802.3ad, ACL, QoS and IGMPv1/v2/v3 from day one.		
8	Switch should have Static Routing for IPv4 & Ipv6 from day1.		
9	Should support 1K IGMP Groups.		
10	All Ethernet Ports should be PoE & PoE+ enabled with 370W PoE Power budget.		
11	Should support 8 queues per port and security protocols like RADIUS, TACACS/TACACS+, AAA & SSH.		
12	Switch should be quoted with 5 years direct OEM TAC support and Next Business Day hardware shipment.		
13	Hardware of the switch should be EAL2 / EAL3 / NDPP certified from Day1		
14	Equipment should be minimum TEC certified or IPV6 Ready Logo Certified. IPV6 Routing & Management features should be active from Day-1.		

Make: **Model:**			
Sl#	**Requirement**	**Compliance (Y/N)**	**Remark (If any)**
15	Comprehensive Onsite OEM Warranty for 5 Years		
16	All the required licenses for making the Switches fully functional should be bundled		
17	The Switch should support IEEE 802.3az standard		
18	Switch OEM must be in 'leaders' or 'Challengers' in the Gartner Magic Quadrant for wired & wireless networking latest published by Gartner.		
19	Comprehensive OEM Warranty for 5 Years		

11.3.4. Network Management System (NMS)

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
	General Requirements		
1.	The solution OEM should have R&D Center in India.		
2.	The solution should be in leader's quadrant in any of the Gartner/Forrester/Research in Action reports in last 5 years.		
3.	The solution should be integrated with software defined WAN (SD-WAN) solution and Digital asset management solution, to be implemented in future.		
4.	The proposed platform should suppoer AI & ML capabilities		
5.	The proposed solution should be modular, scalble and have extensible architecture for scaling-out/in and scaling-up/down.		
6.	Proposed solution should support a distributed architecture for service assurance.		
7.	The proposed solution must have been implemented in any SWAN project across India.		
8.	The OEM must have onsite support system with its Certified manpower.		
	IT Network Discovery & Monitoring		
1.	The solution should be able to do a complete discovery of IT environment across distributed (i.e., physical, virtual, network, application) and heterogeneous environment and provide a clear and visual mapping of IT infrastructure to business services.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
2.	The solution should automatically group servers that work closely together based on analysis of communication between them, automatically build visualizations that shows configuration dependency between switches, routers, physical/virtual host, software, business applications and other entities.		
3.	The data should be fully auditable as to where it came from and what was the method to retrieve that data, show exactly how the discovery data is obtained (i.e., Audit trail and mechanism to validate the quality of data discovered).		
4.	The solution should come with real-time dashboards that collate and present data that allows organizations to make decision on consolidation, re-use of infrastructure, detecting infrastructure that has never been used etc., automatically detect software that are end of support, end of extended support, capture and report on infrastructure drift.		
5.	The solution should perform Application dependency mapping. The solution should include out-of-box extensions for SAP, J2EE, Exchange, Storage, etc.,able to do Virtual systNMS discovery (including VMWare, Microsoft Hyper-V, Solaris, AIX, etc.), have ready made Dashboard that helps in taking decision around server consolidation, software standardization and software license management.		
6.	The solution should have a CMDB that can store the detailed configuration as well as the relationship information between the infrastructure components, have Common Data Model that unifies the representation of configuration data and handles all types of Configuration IT NMS (CI), should have one single CMDB.		
7.	The CMDB should have the Reconciliation facility that should use configurable business rules to merge data from both vendor and third-party discovery tools into a single, reliable dataset, eliminating data overlap gaps, and conflicts between multiple discovery tools and existing CMDB data, CMDB should have federation capabilities. The federated data model provides a single, logical data store that can reside on multiple data sources throughout an IT organization.		
8.	The CMDB data should be used by other consuming applications such as Change Management, Incident Management, Configuration Management etc.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
9.	The CMDB solution should have definitive software library, CMDB should provide a CI Browser and graphical CI Relationship Viewer that allow any IT process users to launch a view into the CMDB to quickly view CI and relationship data relevant to their needs.		
10.	The solution should provide Service blueprints to describe functional and deployment models for the Service definitions, create adhoc reports, charts, and graphs and populate CMDB natively without integration. It should support service modelling which can be started at any point in an infrastructure and therefrom it can be built in an automated way.		
11.	The discovery solution should be an agentless solution so that there is no agent overhead on target servers for discovery.		
12.	The discovery solution should have provision to be deployed in a cluster environment for high-availability and scalability.		
13.	The solution should be capable enough to start application mapping from any point in the infrastructure.		
14.	The solution should identify devices which are not part of an application, is not running any software or is not communicating with other devices.		
15.	The solution should be capable enough to perform event driven discovery for any event occurring, in agentless manner without need to install any agent on any target machines.		
16.	Discovery should work without requiring agent installation (that is, agent-less discovery) while discovery Layers 2 through Layers 7 of OSI model.		
17.	Should use Industry-standard protocols such as WMI, SNMP, JMX, SSH to perform discovery without requiring the installation of an agent.		
18.	Discovery system should have ability to modify out-of-box discovery scripts, create customized discovery scripts.		
	NMS Server Infrastructure Monitoring		
1.	Proposed NMS solution OEM must be ISO 20000, ISO 27034-1 & ISO 27001 certified to ensure service & security compliances.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
2.	The proposed NMS tools must be able to monitor end to end performance of Server Operating SystNMS & Databases and Should be able to manage distributed, heterogeneous systNMS – Windows, UNIX & LINUX from a single management station.		
3.	The proposed NMS solution should be an integrated, modular and scalable solution to provide comprehensive fault management, performance management, traffic analysis and business service management, IT service desk\ help desk \trouble ticketing system & SLA monitoring functionality.		
4.	Proposed solution should have Out-of-the-Box connectors/ probes to integrate with multiple NMS solutions, including industry standard solutions from Micro Focus, IBM, CA, Microsoft etc., and should also provide mechanisms (XML, APIs etc.) to integrate with other NMS and NMS solutions, to provide an integrated topology and event views and reports to the operator.		
5.	The solution should have self-monitoring ability to track status of its critical components & parameters such as Up/Down status of its services, applications & servers, CPU utilization, Memory capacity, File system space, Database Status, synchronization status between primary and secondary system and event processing etc. It should provide this information in real-time through graphical dashboards, events/alarms as well as in the form of historical reports.		
6.	The solution should provide agent-based and agent less monitoring through a single elementary manager – with will allow to choose the level of management required and deploys the right-sized solution to meet those requirements.		
7.	The solution should have the capability to remotely upgrade the agents on target machines without login or reinstallation. It should not be dependent on other solution to upgrade agents.		
8.	There should be a single agent on the managed node that provides the system performance data, and for event management it should be able to prioritize events, do correlation & duplicate suppression ability to buffer alarms and provide automatic actions with capability to add necessary annotations.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
9.	The solution should be capable to do following monitoring for Databases (RDBMs): i. Buffer pools ii. Locks and other details about lock iii. Resources iv. Tablespaces/Datafiles/Logfiles/ Data Usage v. Monitor Health of the SQL server agent and its jobs. vi. Monitor the performance of SQL Server instances against the defined performance counters and usage of different system resources by SQL Server. vii. Monitor Concurrent user, disk latency, cluster system etc. viii. Deadlocks on instances.		
10.	The solution should provide detailed event and performance data reporting with provision for customization of reports.		
11.	The solution should have readily available orchestration workflows for scenario's like Disk Full, Host Down, server not responding, DB Table space Full etc. which can be triggered manually or automatically.		
12.	The solution should be able to monitor the performance of physical devices (like servers), virtualized environment (like Virtual Machines), database and applications through an integrated manager of managers solution. The monitoring systNMS should have APIs that allow easy integration with third party tools. These should include SNMP adapters, parsing log file, TCP/UDP Client Server, Telnet Adapters, Windows Event logs, Command line, C APIS, Web Services API, Perl Interface.		
13.	The solution should be able to correlate events from different elementary managers through a topology perspective for the business services models to do impact analysis for the services. It should provide ability to relate infrastructure topology to business services.		
14.	The solution should have the ability to automate probable cause analysis by automatically grouping events together based on the time that they occur, the business service that they affect and then relating the two to the normal/abnormal behavior of each performance metrics to identify the likely cause of downtime.		
15.	The unified monitoring solution should have mobile app to get alerts on mobile and have a view of infrastructure alerts and business services.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
16.	The solution should have capability to automatically create dynamic base lining for the key performance indicators and have the granularity to learn behavior of key performance metrics per hour, per day, per week basis to reduce false positives.		
17.	The solution must provide a unified event management/ aggregation and reporting dashboard to consolidate all events from various sources to a single view manager.		
18.	The solution should monitor infrastructure, and middleware together - Take an infrastructure -centric view by combining monitoring for servers, databases, storage and other infrastructure technologies.		
19.	The solution should understand the service impact of events - Collect events and create service impact models that visualize the health of services to prioritize problem resolution.		
20.	The system must support multiple built in discovery mechanisms for e.g. Active Directory, Windows Browser, DNS with capability to discover and must be highly scalable to be able to monitor thousands of servers in data Centre.		
21.	The proposed solution should have the ability to forecast and model changes in service demand so that IT can easily adjust the infrastructure resources based on peak, cyclic, or growth in demand, optimize resources with complete visibility for infrastructure services.		
22.	The system should integrate with Helpdesk / Service desk tool for automated incident logging and also notify alerts or events via e-mail or SMS.		
23.	The solution should provide reports for any virtualization platform		
24.	The proposed solution should be able to gather data for all of the infrastructure resources that are important for application and service performance.		
25.	The proposed solution should have the ability to allocate and schedule needed IT infrastructure resources for day-one use so that the IT has a view of both realized and utilized IT resources and thereby IT can plan for onboarding or infrastructure acquisitions.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
26.	The solution should be capable to do following monitoring for servers: i. Disk Failure and Utilization ii. CPU Failure and Utilization iii. RAM Failure and Utilization iv. Event Logs v. OS – Services, Processes etc. vi. Disks: RAID controllers, hard disks, RAIDs (failure prediction, availability of the volumes, etc.). vii. Environment: temperature, internal voltages, power supplies, fans viii. Critical components: processors, memory modules (ECC errors, failure prediction, etc.).		
27.	It should have capability to perform cross domain correlation with alarm correlation from Network Monitoring tool, SystNMS monitoring tool and other domain monitoring tools.		
28.	The solution should leverages one or several sources (manufacturer-specific hardware agents, standard management technologies, SSH, SNMP, WBEM, WMI, etc.) to gather hardware information for harware monitoring of servers.		
29.	The solution should maximize the production value of the assets over time by capturing change at its source, facilitating timely on boarding of equipment at the time of receiving through to the decommissioning of the older equipment.		
30.	The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.		
31.	The solution should be single source of truth for all assets sharing information between facilities, IT and business system.		
32.	Alarms should be mapped to the live topology views and real time updates to topology based on alarm occurrences.		
33.	The solution should predict and forecast the future state of Data Center's physical capacity based on consumption. It should use what-if models to forecast the capacity impact of data center on space and networks.		
34.	It should provide audit and compliance reports for the OSWAN network assets.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
35.	It should help in identifying the improvements required in services and cost saving by extending IT Service Management		
36.	There should be a single agent on the managed node that provides the system performance data, and for event management it should be able to prioritize events, do correlation & duplicate suppression ability to buffer alarms and provide automatic actions with capability to add necessary annotations		
37.	Solution should provide alarm correlation and facilitate reduction of total number of alarms displayed by means of intelligent alarm correlation, suppression and root cause analysis techniques built in to the system. The system must ensure reduction in MTTR by means of advanced event correlation, filtering and root cause analysis.		
38.	The proposed Alarm Correlation and Root Cause Analysis system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The current performance state of the entire network & system infrastructure shall be visible in an integrated console.		
	IT Network Fault Management		
1.	This system shall provide fault, performance and configuration management for multivendor IP Network and must monitor performance across heterogeneous networks from one end of the enterprise to the other.		
2.	The system shall minimize maintenance and administrative tasks by sharing a single inventory database for tasks of monitoring of inventory, performance and faults. Administrators and power users should not be required to populate multiple databases and keep them in sync.		
3.	It shall manage network devices that can be discovered by IP address, link level address, or devices that run IP and Web servers. System shall take up the fault detection & health monitoring of Various Network elements from the device level to the protocol and interface levels. It shall also provide network performance data & threshold based alerts for real time performance monitoring, Service Level monitoring, reporting and historical trending		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
4.	The proposed solution shall automatically discover manageable elements connected to the network and map the connectivity between them.		
5.	The system should provide discovery & inventory 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.		
6.	At the lowest level, network communication shall be done through SNMP V-1, V-2 & V-3 based on the SNMP version supported by the device. System shall process and obtain, automatically, meaningful information such as network discovery and layout of the Network and event handling.		
7.	The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e. Router, Switches, LAN Extender, Servers, Terminal Servers, Thin-Client and UPS etc.) and map the connectivity between them with granular visibility up to individual ports level. The tool shall be able to assign different icons/ symbols to different type of discovered elements. It should show live interface connections between discovered network devices.		
8.	The system must be able to support mapping and modelling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments		
9.	The system shall support maps grouped by network topology, geographic locations of the equipment's and user group/ departments.		
10.	NMS should be able to discover & map graphically the routing protocols in use, such as OSPF areas, etc. There should be provision for automatic/ initiated updates from time to time.		
11.	The system shall provide information regarding capacity utilization and error statistics for WAN links.		
12.	It shall be possible to reduce the set of displayed devices in the topology views by flexible rules, based on the attribute contents stored with each device.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
13.	The system shall support concurrent multi-user access to the management system, enabling multiple read- write access to different areas of the management domain. Visibility and security architecture shall be maintained and administered across the entire distributed domain.		
14.	The system shall be able to support migration to SNMP v3 and/ or latest version to provide added security.		
15.	System shall be able to accept events from all types of elements in the IT infrastructure including network devices, Server's hardware, software, operating system, database, application, storage, security devices etc.		
16.	The system must provide user-configurable discovery control to manage the frequency and scope network discovery, configured using a graphical user interface.		
17.	System shall process events using consolidation, filtering, normalization, enrichment, correlation, and analysis techniques. Then it shall notify the appropriate IT operations personnel of critical events. System shall also automate corrective action wherever possible.		
18.	NMS should support Industry-leading support for physical, virtual, and all type of SDN-enabled devices.		
19.	Tool should support automated Change Plans including but not limited to: Conditions to validate, Pre-Change Validation, Change Script (similar to legacy Command Script), Post-Change Validation, Rollback Script.		
20.	NMS should provide integrated fault, performance Monitoring, Configuration & compliance Management together in one tool.		
21.	NMS should support out of the box monitoring of at least 5000+ devices from at least 150+ vendors.		
22.	NMS should have built-in audit and compliance policies for industry best practices/ Gov. regulations like PCI, HIPAA, NERC and others.		
23.	The tool shall be able to discover IPv4, IPv6 as well as devices in dual-stack. In case of dual stack devices, the system shall be able to discover and show both IPv4 and IPv6 IP addresses.		
24.	The proposed Network Fault Management solution must support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
	Trap based discovery. It must also allow for inclusion and exclusion list of IP address or devices from such discovery mechanisms.		
25.	The alarm collection layer should support resync capability for event collection from NMS.		
26.	Fault management application should have Auto scale-in / scale-out capabilities to dynamically reallocate resources for virtualized fault management as needed.		
27.	The solution should be cloud enabled with containerized standalone director for all micro-services		
28.	The solution should have Common BUS based architecture for persistence and better throughput		
29.	Supplied U-NMS system shall support north bound CORBA/XML/ Q3/SNMP or any other acceptable open standard interface for ensuring integration with other existing/upcoming NMS of similar nature.		
30.	The collection micro-services shall be capable of collecting data from any of the following sources without limitation: xNFs, VIM, NMS, VNFM, SDNC, message bus, controllers and managers, etc.		
31.	For alarm collection layer the HA should be built in within the application.		
32.	The solution should have Common BUS based architecture for persistence and better throughput		
33.	The solution shall support both real-time streaming and batch collection.		
34.	The System shall be able to recognize duplicate alarms by comparing incoming alarms to those already in the current problem list for the reporting object, based on one or more alarm attributes (for example, object name and notification identifier), and automatically suppress such alarms.		
35.	The function shall allow resynchronization with NMS for System alarm status to the current status of the managed equipment.		
36.	The system shall generate alarm for any synchronization issue with NMS. It should also report for services affected due to synchronization in network.		
37.	Fault management application should have Auto scale-in / scale-out capabilities to dynamically reallocate resources for virtualized fault management as needed.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
38.	It shall implement a remedy that eliminates any alarm status discrepancy that may have occurred during operation between the alarm status as presented in System and the real equipment status		
39.	Alarm resynchronization may be necessary in situations such as: i. Equipment failure preventing alarm reporting (for example, disconnection, power failure, hardware defects). ii. Mediation device failure preventing alarm reporting. iii. Data communication link failure. iv. Equipment registered for the first time, but starting with one or more initial alarms. v. Human errors in operation of equipment or System		
40.	The function shall handle ISO-formatted alarms: Communications Alarm, Quality of Service Alarm, Processing Error Alarm, Equipment Alarms and Environment Alarm.		
41.	The function shall handle both notification type events and configuration type events raised by equipment or applications.		
42.	The System shall provide a function that enables faults that occur in the network to be related to the services and circuits that are carried by faulted facilities.		
43.	Alarms arriving at the System shall be transformed into a common format prior to processing by the System. The System should use the common alarm format in all internal System data stores, and in engineer displays, so that external applications that need to process alarms will only have to deal with a single format, and operations staff will see only one representation for all alarms from all network element types.		
44.	The common alarm format supported by the System shall contain at least the following information:- i. Event type. ii. Managed object identifier. iii. Date and time of alarm emission. iv. Perceived severity. v. Probable cause. vi. Notification identifier or correlated notification identifier. vii. Specific problem.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
	viii. Label / Native NMS Name of the Managed Object		
45.	The solution shall provide a threshold cross analytics and detection function.		
46.	The solution shall support the ability to deploy and make use of analytics applications to infer or predict assurance situations. The product shall support integrating AI/ML tools and capabilities to help predict capacity, performance, and other vulnerabilities.		
47.	The solution shall support Complex Event Processing, Root Cause Analysis and Service Impact Analysis capabilities.		
48.	The solution shall support stitching of the performance data for services spanning different domains		
49.	The solution shall support the ability to provide pluggable configuration/utility files which help processors convert custom event types into a standard format (e.g., a mapping configuration file which drives the conversion of custom SNMP events into standard events understandable by the analytics engine)		
50.	The solution shall support the ability to publish the collected data to third party application.		
51.	The solution shall contain a correlation engine with the ability to create and manage correlation rules (i.e., CRUD).		
52.	The System shall provide a comprehensive alarm correlation facility which shall be used for following primary purposes:- i. To determine the root-cause underlying sets of alarms and report the root-cause as a single alarm. ii. To assist in reducing the number of alarms seen by engineers to the minimum necessary to effectively manages the network. iii. The correlation function shall correlate large number of alarms to identify the underlying problNMS affecting the network equipment. iv. The function shall be used to automate network management tasks. In particular, it shall be used to perform high-level automated actions for Alarm filtering, Alarm aggregation, Alarm enrichment, Root cause analysis and Service impact analysis.		
53.	It shall support collection, filtering, recording (logging of the actions performed on the alarms), storage, and correlation and management functions.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
54.	The stored alarm records shall be made available to, and managed by, other System applications in real-time.		
55.	The “terminated” alarms shall be exported to a database for further user-defined processing.		
56.	The System shall be able to automatically clear an outstanding alarm when a corresponding clear-alarm is received (corresponding means that the managed object name and the notification identifier are the same in both the alarm raise and the alarm clear, and that the clear was emitted temporally after the raise).		
57.	The system shall support configuration of threshold for data polling (alarms) to make sure CPU utilization is not exceeded the permissible limit, because data polling keeps on consuming CPU as the alarm count increases.		
58.	The products as listed above must have been deployed in a Telecom Project and should have been in successful operation (accepted by customer) for at least three (3) years as on the originally scheduled date of bid opening		
59.	The System shall support at least the following alarm states (or their equivalents by other names): - i. Raised (an alarm has been raised but not yet acknowledged) ii. Acknowledged (an operations staff has acknowledged that they have seen an alarm). iii. Handled (handling of an alarm has been started). iii. Cleared (the condition that caused an alarm to be raised has been cleared). iv. Archived (an alarm has been archived and is eligible to be purged from local storage).		
60.	The System shall support multiple alarm-display domains. It shall be possible to apply filters to each alarm-display domain so a given domain shows only a selected subset of the total list of outstanding alarms.		
61.	Consolidated Fault management system should enable operators to Identify hot spots and frequently occurring events with guided search based on best practices. The search should be based on key words and should fetch data from real time as well as historical events for empowering operators with relevant and quicker Root Cause Analysis.		
62.	The system shall have report generation facility for RCA and alarms elementwise, link/service wise/ port wise etc.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
63.	The system shall take in to consideration all standard protection mechanisms while computing the RCA.		
64.	The system shall be able to modify the RCA results on receiving every/new alarm from the network.		
65.	The system shall have capability to correlate and display the relationships across Root		
66.	The solution to maintain an internal view of end-to-end service topology, including the service decomposition as well as the connectivity details.		
67.	The solution to support the ability to integrate with a 3rd-party topology system/database.		
68.	The solution to provide northbound APIs for retrieving the topological information for other components to consume.		
	IT Performance Management		
1.	System shall Collect, analyze and summarize management data from LAN/WAN, MIBII interfaces, various systNMS and services for performance management. It should allow identifying trends in performance in order to avert possible service problNMS.		
2.	System shall provide availability, service levels, response time and throughput of various Internet/ web services e.g. DNS, HTTP, SMTP etc.		
3.	System shall provide Performance of Network devices like CPU, memory & buffers etc, LAN and WAN interfaces, Network segments and VLANs.		
4.	The proposed system shall identify over-and under- utilized links and assist in maximizing the utilization of current resources		
5.	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: a) Capture running configuration; b) Capture start-up configuration; c) Upload configuration; d) Write start-up configuration; e) Upload firmware		
6.	The proposed system shall provide easy to read representations of health, utilization, latency and availability.		
7.	It shall provide reports through web, and also generate “pdf” / CSV reports of the same.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
8.	It shall give user flexibility to create custom reports, on the basis of time duration, group of elements, custom elements etc.		
9.	System shall provide reports through e-mail to pre- defined user with pre defined interval.		
10.	System shall provide web-based reports both near real time and historical data for the systNMS and network devices.		
11.	System shall reports per Server, Application, infrastructure services and Network devices in CUSTOMER environment.		
12.	It shall provide Real time network monitoring and Measurement of end-to-end Network/ system performance & availability to define service levels and further improve upon them.		
13.	Detailed analysis of performance metrics and response time for the network shall be made available.		
14.	System shall identify how device resources are affecting network performance, document current network performance for internal use and service level agreements (SLA).		
15.	Executive Summary report that gives an overall view of a group of elements, showing volume and other important metrics for the technology being viewed.		
16.	The system should identify underutilized servers – both physical and virtual – providing the necessary metrics to assess utilization. Metrics should include server name, management IP, CPU utilization, Used Memory, number of processes, number of users, and a normalized average ranking.		
17.	Service Level report that shows the elements with the worst availability and worst response time-the two leading metrics used to monitor SLAs.		
18.	The proposed system must have a built-in report authoring tool which will enable complete customization flexibility of performance reports.		
19.	The tool should provide an integrated performance view for all the managed systNMS and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
20.	It shall be possible to put logo on reports and arrange or change tables and graphs to meet requirements.		
21.	The system should provide a set of reports or UIs that allow non-technical audience such as Line Of Business managers understand how network supports their business needs or not, and how network outages affect availability of their applications.		
22.	It should be easy to retrieve current and historical inventory, performance and faults data from the system for custom data mining and reporting purposes.		
23.	For simplicity of use, fast learning curve and minimized maintenance and usage costs, the system should provide users with a single user interface, with a single reporting engine and with a set of reports that combine inventory, performance and fault data for added-value reports.		
24.	The system should provide a set of reports that allow quick comparison of performance and errors of critical interfaces (individual/aggregated) and their correlation with utilization of hardware resources of their devices.		
25.	The system should be able to identify and report on ports per device not currently being utilized including the date/length of time since last activity. Statistics/reports should be available by customizable logical grouping to adequately represent network segments.		
26.	The system should identify and report on device power utilization at the device and port level. Reports should allow easy prioritization of devices consuming the most power.		
27.	The system should allow creation of policies to configure, track, and report on sustainability initiatives to lower overall power utilization. It should include user customizable groupings to simplify tracking and reporting to business units or company divisions.		
28.	The system should be able to clearly identify configuration changes / policy violations / inventory changes across multi-vendor network tool.		
29.	The system should enable comparison and reporting of key device operational attributes across multiple ports on different devices. For example, the system should be able to compare port inbound utilization of select ports on several different devices.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
30.	It shall be able to monitor and report on availability, delay of target IP nodes – i.e. router interfaces - and also monitor and provide reports on historical utilization of CPU, memory of critical monitored servers running SNMP and management agents.		
a.	Trend Reports		
b.	Ad-hoc reports		
c.	Top N Utilization Reports		
d.	Capacity prediction Reports		
e.	Availability Reports		
f.	Availability, Uptime & Downtime for both Link and Device - Daily, Weekly, Monthly, Yearly Basis		
g.	Trend Report		
h.	Top N report		
i.	Custom report		
j.	Performance Reports		
k.	CPU and Memory utilized		
l.	Interface errors		
m.	Server and Infrastructure services statistics		
n.	Trend report based on Historical Information		
o.	Top N report		
p.	Custom report		
q.	SLA Reporting		
r.	Computation of SLA for entire CUSTOMER Infrastructure		
s.	Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports		
31.	The system should include both static and dynamic thresholds for key operational attributes on devices and ports. Thresholds should be customizable/overridden by logical group, device type, or individual device/port level.		
32.	The system should support secure device configuration capture and upload and thereby detect inconsistent “running” and “start-up” configurations and alert the administrators.		
33.	Reporting solution should be able to report on Service Level status of configured business service.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
34.	The system should use same and single application instance for network performance, configuration deployment and compliance management of network devices and solution has to be deployed in VMs.		
35.	The solution shall use single database for tasks of monitoring of inventory, performance, fault, reports etc.		
36.	The solution shall provide availability, service levels, response time and throughput of various Internet/ web services e.g. DNS, HTTP, SMTP etc		
37.	The system should not use separate smart plug-ins to generate reports related to QoS, MPLS and it should be availble out of the box with the solution.		
38.	The system should support to utilize the IPv6 Neighbor Discovery (ND) protocol, with Maps including the IPv6 ND link type.		
	IT Service Management		
1.	The solution should have Service Management documentation/ guidelines in built based on latest ITIL best practices and must be ITIL 2011 Gold-level certified on at least 10+ processes by Pink Elephant for process like Incident management, Problem Management, Change Management, Knowledge Management, Service Level Management, Service Asset and Configuration management, Service Catalogue and Request Fulfilment, etc. The certification copy to be submitted.		
2.	The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost center, and user role for Incident, Problem, Change, Release, Knowledge Management, Asset Management and CMDB.		
3.	Service Management solution OEM must be an industry standard, enterprise grade solution and shall be in the present in Leaders Quadrant of Forrester / Gartner / IDC report for ITSM for the last two years.		
4.	Provide the ability to develop workflow for data level operations like record create, update, modify and delete operation. Workflows could be executed for Web client.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
5.	Provide option for approval engine so that any customized applications developed could incorporate the hierarchy, role based, level based ad-hoc approval structure. Include notification and escalation capability if approval is not performed.		
6.	The solution should provide the functionality of executing searches to the entire database. It should be possible to provide query criteria using AND, OR conditions. This allows the users to create and view workflows/reports based on their needs rather than using only the set of workflows/reports provided out of the box.		
7.	An interactive service management process model -		
8.	Enforcement of best practices via process flows, workflows, and task flows.		
9.	The solution should have the ability to operate all functionality available in the incident, problem, change, assets etc. via a mobile device like iPhone, Android phone, blackberry etc.		
10.	The solution should have the capability to automatically create a copy of the ticket to an archival server based on conditions like after a particular date or every ticket/change or assigned to a particular group etc.		
11.	The solution should provide email based interactions allowing ticket creation,update and approval of request.		
12.	The support person can interact with the end users through chat in built and add those chat transcripts in the ticket.		
13.	The solution should give all the details related to a particular business services.		
14.	The system should have graphical interface to define, visualize and update ITIL processes.		
15.	Should support single service catalog for end users to submit and track service request, spanning both IT services and non-IT services.		
16.	Should provide for Service Requests Workflows and Fulfillment definitions for commonly used IT/non-IT services.		
17.	Centralized Self Service Portal – One architecture supporting all users; internal, external and private-public-hybrid clouds.		
18.	Catalogue based on User role – enables access to service request on user role.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
19.	The solutions should allow effectively creating and managing a shared services catalogue for all service request with flexible entitlement controls. The solution should have wizard / graphical workflow editors allowing definition pf new request in minutes – without any programming.		
20.	Various types of Customer profiles are supported, for ex: Gold, Platinum, Silver.		
21.	Integrates with any underlying service management including Service Desk, Change Management, Service Level Management and CMDB for request fulfilment.		
22.	Tool Analytics should be completely configurable in terms of source data and results, enabling Process Managers and other IT Users to proactively identify trends that can be used to drive action. Multiple instances shall be allowed to be configured in different ways in different modules for different outcomes - for example one should be able to identify trends in one set of data and subsequently develop linkages with other data, or Analytics can run on top of reporting results to provide further insights from unstructured data.		
23.	Ability to position both Custom-made and Standard Requests.		
24.	Should send notifications to Customers based on the status.		
25.	Should have the ability to extend and create new service request.		
26.	Should have catalogues that cover standard and non standard IT and other services.		
27.	The services should be integrated to SLAs and should be auto measured for adherence.		
28.	The Service catalogue should have a built-in knowledge base for faster issue resolution		
29.	The solution should have out of box catalogue for common request like IMAC, configure mail box etc.		
30.	Users should be able to request for services on behalf of other employees and the system should track the request as if the request has been initiated by the user requesting for the service.		
31.	The service catalogue should be searchable.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
32.	The solution should provide advertising space in the portal to inform users about new schemes or new services launched by IT.		
33.	Beyond mobile iOS and Android apps, Self Service App should be available on any device with an HTML5 browser.		
34.	Should support iOS, Android and Desktops.		
35.	Self-service app that reduces IT friction, cuts support costs, and boosts customer satisfaction.		
36.	Context-Aware Services with alerts and service updates.		
37.	The solution should provide a snapshot of day, displaying activities feed with upcoming appointments, pending requests, unresolved issues, and alerts from systNMS used in daily work.		
38.	The Knowledge Management solution should be available in a Multi Tenanted environment.		
39.	Should provide out-of-the-box categorization, as well as routing and escalation workflows that can be triggered based on criteria such as SLA, impact, urgency, CI, location or customer.		
40.	The tool should have the knowledge management OOB – knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions.		
41.	The tool should allow the creation of different access levels (i.e. Read only, write, create, delete) to knowledge management system.		
42.	Knows users role, location, preferences, and equipment.		
43.	App should allow discovery and mapping of assets.		
44.	Users should be able to add assets to the location-aware floor maps with drag-and-drop ease.		
45.	Service Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged for IT and non- IT services.		
46.	Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.		
47.	The solution should provide embedded and actionable best practices workflows i.e., best-practices process & views based upon implementations.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
48.	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.		
49.	Should able to support and handle large volume of incident, service requests, changes, etc... and should able to integrate with third party IVR or CTI.		
50.	It should be possible for L1 to view the 'Health of a selected asset' from within the ticket. The health view should be consistent across platform (Windows & flavours of UNIX).		
51.	It should have the ability to search multiple built-in knowledge bases like the incident, problem, known- error database simultaneously without requiring the agent to search each knowledge base individually.		
52.	Should support automatic assignment of ticket to the right skilled resource based on business priority Ex - Database crash issue need not be assigned to an L3 DBA unless the business service is completely down		
53.	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues. Should support full text search capabilities.		
54.	For integrations with other NMS/NMS tools, various options for integration should be provided - APIs, web services, SDKs.		
55.	Should Centralize all known error and problem workarounds into a single, searchable knowledge base.		
56.	The tool should allow the user to take a screenshot of the error message and sends it to the service desk. The user can type in a couple of text lines to describe the error in simple language. The service desk agent then can pick up the ticket with the information already filled in (category, impact, and assignment).		
57.	It should provide an interactive process flow bar that guides novice users through the ITIL process for incident management to ensure faster recording and issue resolution.		
58.	The incident Management solution should be completely integrated to the CMDB to ensure that CIs can be associated with the ticket to provide better visibility L2 agents.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
59.	The incident management solution have the ability to initiate the change request on a button click.		
60.	The solution should have the ability to associate an incident with an existing change request, a problem or an known error for tracking purposes.		
61.	Service Desk should able integrate with Mobility solution for quick and easy access to address reported issues.		
62.	The solution should be able to track a request for change through the different stages of lifecycle of a change request.		
63.	The tool should facilitate the identification of the change type and associated workflow For example: standard, normal, and emergency.		
64.	The tool should facilitate the differentiation of normal Changes For example: Category - Minor or Small, Category - Significant or Medium, Category – Major or Large.		
65.	The tool should facilitate the ability to create simple to complex request workflows through sequential and parallel tasking.		
66.	The tool should notify all the users about the scheduled changes/outage and sent a reminder to responsible contacts for implementation of change.		
67.	Change management should have fields to record impact analysis and simulate impact, back-out plans, within the change record.		
68.	Service Impact simulation and collision detection - It should have the capability to automatically and continually perform impact analysis, risk assessment, and change collision dates detection (for same CI's) on all change requests. The solution should provide complete view of planned changes with services & their components.		
69.	The tool should facilitate the scheduling of post implementation reviews for implemented changes after defined time interval.		
70.	The application should have the ability to assign change advisory board (CAB) responsibilities to change management roles.		
71.	The tool should facilitate ability of authorized roles to reject changes For example, status of reject, ability to record reason for rejects notification.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
72.	The change approval engine should be configurable such that approvals can happen if either one of the individuals approve a change, or a majority approve the change, or certain people in the committee approve the change etc. It should also incorporate multi-staged approvals like manager, Sr manager, CxO etc.		
73.	Change management should be capable of integrating with CMDB to facilitate access to CI attributes and relationships to enable change assessment and authorization.		
74.	The solution should allow the identification of post implementation impact and resource utilization for completed changes, track incidents and problNMS resulting from an implemented change, further enable analysis of planned versus actual resources utilized for change.		
75.	The solution should have Unified and uniform approach to enterprise change and release management across infrastructure, enabling organizations to automate best practices for asset change management with enterprise-wide change control and release management processes.		
76.	Solution should provide a consolidated view of the tasks that the release management team must perform to drive the completion of the change requests and activities required to close the release.		
77.	Solution should provide Change and Release Calendar views for the current schedule of releases, change requests, and business events for any potential conflicts.		
78.	Solution should provide the ability to analyze the impact of change to the appropriate non-IT business services and IT services.		
79.	The solution should have the ability to prompt change planners with suitable time slots for conducting a change depending upon the changes that have been scheduled/in progress, risk associated with it and the priority of the change.		
80.	The solution should have the ability to identifying and flagging changes that are being done by various team to prevent change collisions.		
81.	Release management solution should provide ability to assign change task to implementer for deployment.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
82.	The tool should integrate with knowledge management OOB - knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions.		
83.	The tool should allow the creation of different access levels (i.e Read only, write, create, delete) to knowledge management system.		
84.	The tool should allow creation and enforced use of data input rules for creating knowledge records For example: mandatory fields for content and information; QA and change approval to move from draft to production.		
85.	The tool should automate the population of knowledge records with author and owner data, creation date, as well as any other attributes required by organization		
86.	The tool should facilitate the identification of redundant or duplicate information, whether in single record or multiple records		
87.	The Knowledge Management solution should be available separately in a Multi Tenanted environment.		
88.	The tool should automate trending of knowledge use & identification of knowledge gaps.		
89.	The tool should allow automating notification to interested parties on submission new knowledge/solutions applicable to them.		
90.	The tool should have a powerful search engine to sort, retrieve and search using advanced search options, search content in multiple format, and also search within knowledge records.		
91.	The tool should automate the creation of a request for change or service request when a knowledge record needs to be modified.		
92.	The tool should allow displaying FAQs and highlight the newly added knowledge content.		
93.	The module should allow integration with all other modules of service management to enable knowledge records to be quickly created from records with associated links.		
94.	The solution should have the ability to prompt users with a interactive set of questions and answers that will eventually guide the users to the relevant solution.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
95.	The module will facilitate opening of a problem record directly from a menu for pro-active tracking of problem activity as well as from an incident record for reactive tracking of problem activity.		
96.	Should Provide a single shared view of services supporting Service Design, Transition and Operations stages of the lifecycle.		
97.	The Configuration Management Database should support multiple datasets with federation and reconciliation facilities so as to get data from various discovery tools and also through manual import process.		
98.	Reconciliation of data should be possible with multiple data providers based on common attributes and ability to define precedence rules on attributes.		
99.	Federation of external data sources should be possible with ability to store common attributes inside CMDB and getting other attributes from external data sources in real time.		
100.	Should automatically create Service models to describe how IT infrastructure supports business services.		
101.	Should Provide a Service catalog so as to establish a framework for Service definitions based on IT and business alignment.		
102.	Should Provide Service blueprints to describe functional and deployment models for the Service definitions.		
103.	The CMDB should have built-in drift management capabilities to capture and report on infrastructure drift based on infrastructure attributes like RAM, memory, etc.		
104.	Solution should support comprehensive SLA management platform that cuts across Infrastructure Management and Service Management. For e.g. monitors and reports across different KPIs like infrastructure (CPU utilization, disk space), response times , resolution times (eg. incident closed on 2 hours) performance and custom parameters of an enterprise		
105.	Have a consolidated, automated graphical report for SLA compliance with ability to drill down to reason for non-compliance.		
106.	Manage service levels for delivery and support of business services.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
107.	Real-time visualization of service level targets, agreement compliance data, penalties and rewards.		
108.	Should support compliance and cost trending to assist in identifying areas for process and operational improvements.		
109.	The service level management (SLM) tool should facilitate creation and maintenance of SLAs, OLAs and Supplier / Underpinning Contracts For example: scope, supplier, contact names, contact method, support hours, service level targets.		
110.	The product should have the capability to schedule the review cycle and renewal of SLAs, OLAs and supplier / underpinning Contracts.		
111.	The module should link available support hours to service levels when calculating deadlines as well as suspend SLA calculation for certain criteria – eg'pending information from customer'.		
112.	The product should facilitate bi-directional linking of services & customers to associate multiple agreements with a customer contract as well as link multiple customers to a particular service.		
113.	The tool should facilitate the production of Key Performance Indicator (KPI) reports as out of-the-box or ad hoc reporting.		
114.	The SLM module should integrate with incident and problem management to automate escalation, and notification activities based on response and resolution targets.		
115.	It should also integrate with change management to provide access to service level agreement details, implementation windows, change blackout periods, and availability requirements.		
116.	The product should support integration with event management and monitoring tools to enable triggering of service support related actions based on established thresholds.		
117.	The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost centre, and user role for Incident, Problem, Change, Release, Knowledge Management, Asset Management and CMDB.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
118.	The solution should provide to browse through CMDB which should offer powerful search capabilities for configuration itNMS and services, enabling to quickly find CIs as well as their relationships to other CIs.		
119.	The Service Desk tool should be capable of operating in a Managed Service model using multi-tenancy functionality to support multiple levels of administrative delegation of different clients		
120.	The service management application should be user friendly, accessible via intranet, internet & mobile devices.		
121.	The service management software should have the ability to tightly integrate (bi-directionally) with enterprise management systNMS for auto-creation/closing / reporting of events/incidents/trouble tickets.		
122.	The tool should have security controls in place to allow only authorized staff and users of different clients to view, open, modify, authorize and close records based on their role.		
123.	The software should have a unique distinguisher to identify the type of ticket.		
124.	The tool should have an option to create tiered categorization structure allowing the identification of a ticket with a service as well as system and component.		
125.	The application should have a predefined/customizable field to indicate & track the progress/status of the lifecycle of ticket(s). It should contain predefined status codes and allow defining new status codes		
126.	The tool should provide an audit trail, tracking & monitoring for record information and updates from opening through fulfilment to closure For example: IDs of individuals or groups opening, updating & closing records; dates / times of status & activities updates, etc.		
127.	The tool should have the ability to notify and functionally escalate (assign) a ticket to an individual or support group based on pre-defined parameters, thresholds or manual override conditions.		
128.	The tool should integrate with a directory system to enable recording and accessing customer records of information.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
129.	The Solution should provide a centralized Dashboard that picks up relevant business metrics from the monitoring and service management solution - Business Perspectives – Business-centric dashboards giving at-a-glance visibility to key operational initiatives.		
130.	The IT organization and business stakeholders should be able to view their tickets by business service and impact from the same solution.		
131.	Solution should have the ability to display the events in a table, service, infrastructure, tree views. It should provide each user the ability to select or view the events as per their convenience.		
132.	Should support advanced filtering to eliminate extraneous data / alarms in Web browser and GUI.		
133.	These dashboards need to be dynamic that allows user to drag and drop these metrics and create custom dashboards without any coding.		
134.	Apart from built-in sections, users should also be able to create custom sections that can reference out to custom metrics stored in the monitoring tools databases or other sources as per the business requirements.		
135.	It should be possible to restrict access to data available in the sections as per the user rights of the users. Profile based data access.		
136.	For each section, user should be able to select the time frame to report on data. This could be monthly, quarterly, half yearly, yearly or custom dates.		
137.	The Dashboards should support rich formatting capabilities to represent the data, this includes different chart formats and PDF.		
138.	The Solution should come with standard report on overall business service health and performance.		
139.	Solution should use unified and seamless architecture and workflow to resolve business issues.		
140.	Solution should use a natively integrated suite of IT service support processes with a single CMDB.		
141.	Solution should have clear integration of service support processes with event management and change execution to create end to end workflows.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
142.	Solution uses integration of operational events to incident and problem process in order to simplify Service Desk operations.		
143.	The solution should have a single CMDB across ITSM and Asset Management system.		
144.	Solution provides a graphical workflow designer that can be used to create SRM fulfilment flows and extend other ITSM processes through configuration		
145.	The Solution should display the complete ITIL process flow for Incident, problem, Change and release, Asset and Service level Management. It should have Service Management Process Model in built based on ITIL v3 best practices and have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost center, and user role for Incident, Problem, Change, Release, Knowledge Management, Asset Management and CMDB.		
146.	The solution should have a single CMDB across ITSM and Asset Management system and it should provide the ability to develop workflow for data level operations like record create, update, modify and delete operation. Same workflow could be executed for both Window and Web client.		
147.	Provide option for approval engine so that any customized applications developed could incorporate the hierarchy, role based, level-based ad-hoc approval structure. Include notification and escalation capability if approval is not performed. The solution should provide the functionality of executing searches to the entire database. It should be possible to provide query criteria using AND, OR conditions. This allows the users to create and view workflows/reports based on their needs rather than using only the set of workflows/ reports provided out of the box.		
148.	The solution should have the ability to operate all functionality available in the incident, problem, change, assets etc. via a mobile device like iPhone, Android phone, etc.		
149.	Should support single service catalogue for end users to submit and track service request, spanning both IT services and non-IT services. Should provide for Service Requests Workflows and Fulfilment definitions for commonly used IT and non-IT services.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
150.	It should be a centralized Self-Service Portal – One architecture supporting all users; internal, external and private-public-hybrid clouds.		
151.	The tool should provide an audit trail, tracking & monitoring for record information and updates from opening through. The tool should have the ability to notify and functionally escalate (assign) a ticket to an individual or support group based on pre-defined parameters, thresholds or manual override conditions.		
152.	Solution should support comprehensive SLA management platform that cuts across Infrastructure Management and Service Management. For e.g. monitors and reports across different KPIs like infrastructure (CPU utilization, disk space), response times , resolution times (eg. incident closed on 2 hours) performance and custom parameters of an enterprise. Have a consolidated, automated graphical report for SLA compliance with ability to drill down to reason for non-compliance. Manage service levels for delivery and support of business services. Real-time visualization of service level targets, agreement compliance data, penalties and rewards.		
153.	Should Provide Service blueprints to describe functional and deployment models for the Service definitions. The CMDB should have built-in drift management capabilities to capture and report on infrastructure drift based on infrastructure attributes like RAM, memory, etc. Should provide Attribute-level normalization and reconciliation to leverage existing data from third-party asset or discovery tools and realize the goal of having one dependable source of configuration data.		
154.	Service Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged for IT and Non IT services. Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels. The solution should provide embedded and actionable best practices workflows i.e., best-practices process & views based upon implementations. It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
155.	The solution should be able to track a request for change through the different stages of lifecycle of a change request. The tool should facilitate the identification of the change type and associated workflow For example: standard, normal, and emergency. The tool should facilitate the differentiation of normal Changes For example: Category - Minor or Small, Category - Significant or Medium, Category – Major or Large.		
156.	The tool should integrate with knowledge management OOB - knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions. The tool should allow the creation of different access levels (i.e Read only, write, create, delete) to knowledge management system. The tool should allow creation and enforced use of data input rules for creating knowledge records For example: mandatory fields for content and information; QA and change approval to move from draft to production.		
157.	Should support compliance and cost trending to assist in identifying areas for process and operational improvements. The service level management (SLM) tool should facilitate creation and maintenance of SLAs, OLAs and Supplier / Underpinning Contracts For example: scope, supplier, contact names, contact method, support hours, service level targets. The product should have the capability to schedule the review cycle and renewal of SLAs, OLAs and supplier / underpinning Contracts.		
158.	It should enable creation, measurement and reporting of three categories of SLA service targets — time-based on response / resolution of tickets, availability relating to uptime of systNMS/ services, or performance- monitoring catering to system metrics.		
159.	The module should link available support hours to service levels when calculating deadlines as well as suspend SLA calculation for certain criteria – eg “pending information from customer’.		
160.	The service management software should have the ability to tightly integrate (bi-directionally) with enterprise management systNMS for auto-creation/closing / reporting of events/incidents/trouble tickets.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
	IT Network Performance Management		
1.	Proposed NMS solution MUST have at least 3 deployments in Indian Government/ Public Sector, monitoring & managing 10,000+ devices (including IT assets - Servers (Physical & Virtual), Network devices, etc.; Non-IT Assets - UPS, KVM, PDU, etc.; Surveillance system - Cameras, Sensors, etc. in each of such deployments. Customer names, solution details and OEM undertaking needs to be provided at the time of bidding.		
2.	Diagnostic Analytics providing change-Correlated Performance Views and should show the difference either in either a side-by-side, or line-by-line presentation.		
3.	The solution should provide real time visibility into top conversations happening in the network and support extensive reporting capability with 1-minute granularity, custom breakdowns (for analyzing flow data by user-selected combination of data types, such as source and destination IP, address ranges, port, protocol, QoS classes, etc.), adjustable data retention settings, flexible grouping controls, and the ability to store years of rolled-up data.		
4.	The solution should provide advance analysis by enabling precise definition of displayed timeframe, either by entering times explicitly or using zoom control to focus on a specific timeframe and allowing traffic to be grouped together by application type and/or IP address range.		
5.	It shall provide key performance monitoring capabilities by giving detailed insight into the application traffic flowing over the network.		
6.	It shall be able to capture, track & analyse traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc.		
7.	It shall be able to monitor network traffic utilization, packet size distribution, protocol distribution, application distribution, top talkers etc. for network traffic.		
8.	It shall collect the real-time network flow data from devices across the network and provide reports on traffic based on standard TCP/IP packet metrics such as Flow Rate, Utilization, Byte Count, Flow Count, TOS fields etc.		
	Reporting and Dashboards		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
1.	The performance management system shall have the ability to provide SLA reports on the following metrics: • Availability (Link & Device) • BW utilization • Resource utilization (in WAN / LAN) • Response Time • Throughput • Latency • Jitter • Loss ratio • Downtime • Failure Frequency • Mean time to repair • Mean time between failures • Uptime (Link and Device) • Error statistics		
2.	The Performance Management shall have user defined set of reports like: a. Summary Reports for specific groups: Reports displaying per group of resources the group aggregations for a set of metrics (for example, per City, the maximum traffic or the total traffic). b. Summary Reports for specific Resources: Reports displaying for a set of resources the period aggregations for the same set of metrics (for example, per interface, the maximum traffic over the day). c. Detailed chart Reports: Reports displaying for one resource and the same set of metrics the values over the period (for example, the raw collected values for the day). d. Resource Threshold Violation Reports: Reports displaying the resources for which a threshold was violated		
	Automation		
1.	Visualizes server, network, storage, and logical application environments and dependencies and compliance state. Provides Layer 2 and virtual LAN (VLAN) network information. Intuitive visual snapshot comparison reduces troubleshooting time.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
2.	Should Detect, collect and maintain information about Managed Servers, including packaged, unpackaged software, runtime state, host/guest relationships and more.		
3.	Defines server build sequences for provisioning, incorporating operating systNMS, patches, and software policies. Supports Solaris, Linux, and Windows®. Supports provisioning of VMware Hypervisor and Solaris Zones.		
4.	Identifies server vulnerabilities quickly and easily and reduces the time needed to patch multiple servers. Enables patch policy creation and flexible patch deployments. Supports native patch formats for all major operating systNMS. Provides out-of-the-box integration with Microsoft® Patch Network and Red Hat Enterprise Linux.		
5.	Enables rapid troubleshooting and configurable compliance management by comparing servers to reference servers, most golden reference snapshots, industry best practices, or user-defined scripts. Provides comprehensive compliance dashboard with consolidated servers and cross-tier compliance views.		
6.	Uses the communications channel with enhanced security features, audit logs, and access control policies to provide direct connections to servers in any location. Supports remote desktop connections, Windows PowerShell, and any shell of Linux environments.		
7.	Solution has ability to integrate with LDAP / Active Directory for user authorization and support audit, annotation for user actions.		
8.	Improves automation efficiency by managing remote systNMS and executing tasks from a command line interface. Also supports Windows PowerShell to provide a command line interface (CLI) to Windows servers.		
9.	Provides dynamic, real-time, and historical reports into hardware, software, patches, and operations activities in complex, heterogeneous data centres. Includes out-of-the-box compliance reports and at-a-glance compliance status with actionable links to servers, policies, and other objects. Exports reports to HTML and comma-separated values (CSV) formats.		
10.	Will support audit and remediation against industry best practice content such as CIS, MSFT.		
11.	Open a remote terminal or get complete server history		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
	directly in the application visualization interface		
12.	System should provide a shell interface to let users operate through a command line across multiple servers simultaneously.		
13.	The network automation solution should be able to retrieve and archive network device configuration files.		
14.	The network automation solution should be able to alert to changes in device configuration files.		
15.	The network automation solution should be able to alert to changes to firmware versions and the automatic retrieval of device configuration.		
16.	The network automation solution should be able to perform “load & merge” configuration changes to multiple network devices.		
17.	The network automation solution should be able to enable detailed comparison of device configuration files.		
18.	The network automation solution should be able to identify trivial changes in device configuration files to be excluded when identifying differences between files.		
19.	The netowork automation solution should be able to check device configuration files for best practice.		
20.	The network automation solution should be able to access devices using Telnet and SSH.		
	User Interface		
1.	The solution shall support both graphical UI and command-line user access points to all exposed functionality		
2.	The GUIs shall support management of the control loops and constituent micro services running on the Service Assurance platform.		
3.	The System Fault Management solution shall provide network engineers a global view of their networks, and enable them to activate management functions and operations from single or multiple workstations.		
4.	The GUIs shall be extensible through plugins to support integration of GUIs provided by third party service assurance applications.		
5.	The GUI shall support graphical visualization of the service instances and their dependencies		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
6.	The GUI shall support drill down on higher-level components to show the low- level details of those components, including visualization of inter-component connectivity.		
7.	The GUI shall support the ability to graphically overlay collected events and metrics on top of the associated service components.		
8.	The GUI shall support the ability to create custom graphical visualizations for services		
9.	The GUI shall support the ability to integrate links to other UIs or portals, such as ability to integrate with any open source visualization tools.		
10.	The FMS window shall display end to end circuit view in a graphical fashion highlighting the affected section.		
11.	Any fault in FMS window should be graphically represented graphical topology/circuit view.		
12.	User privileges and rights should be decided as per requirements. All activities carried out by any user should be captured in the log.		
13.	The system shall obtain the related equipment asset/inventory information and add the inventory information into the alarm information and display the information in the FMS window.		
14.	It shall provide real-time monitoring and notification to allow engineers to handle alarms as they arrive.		
15.	Each alarm-display domain shall be implemented as a Graphical User Interface (GUI) that is intuitive to use and will require minimal engineer training time.		
16.	The alarms displayed in all display domains shall be color coded (customized as per employer requirement) on the basis of perceived severity.		
17.	Engineers should be able to define their own individual set of data that is to be reported against alarms (for example, some engineers may want to see the additional text of alarms, while others may not).		
18.	Map display, with a top-level summary of the current network status in a selected geographic area. The colors of the icons shown on such a display should reflect the current worst alarm status of the underlying elements. Initiating an action against an icon should cause a “zoom-in” to show		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
	progressively more detailed views of the individual lower-order entities that comprise the icon.		
19.	Root-cause domain, in which a selected set of current root-cause alarms is displayed in tabular form. Selecting an alarm and invoking an action against it should show the alarms that contributed to the raising of the root-cause alarm.		
20.	At a given point of time, the system shall be able to list all affected or degraded services in a separate UI with their corresponding root cause alarm		
21.	The system shall be able to show all the lower order trails that are affected when the corresponding higher order trail has failed		
22.	The system shall be able to list the services for every topological link or network element that will be affected or degraded when this element goes down		
23.	The System Notify Function shall support manual or automatic forwarding of notifications via SMS, email. It shall support forwarding of selected alarms to individuals based on configured notification settings.		
	User Authentication & Authorization		
1.	The System shall provide an option for the newly logged in user to change his password and the user shall be forced to change the password first time. It shall also provide option to authenticated user to change password.		
2.	Passwords shall be encrypted and stored in database and will not be stored in clear text.		
3.	Strong Password techniques shall be employed as powerful password login mechanism.		
4.	The System shall provide User account expiry date. It shall be set/modified to the required number of days, once the number of days set for the user account exceeds, the user will not be allowed to log in to system as the user status will be changed as "user Expired". Configuration for the user Expiry shall be enabled or disabled accordingly.		
5.	The System shall allow User login to be enabled /disabled.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
6.	The System shall provide Password expiry date and can also be set/modified as number of days after which the user status will be changed as "Password Expired". By default the password expiry is enabled and set for 90 days. Thus when the user tries to log in, then the message "Password Expired" will be displayed and user is allowed to configure a new password.		
7.	The System shall provide a mechanism in which continuously failed login attempts will be detected and controlled. Number of failed login attempts shall be configurable and will default to 5. After 5 failed attempts, the User account shall be locked. The process for unlocking shall be finalized during detailed engineering. The failure attempts and unlocking of User account shall be logged in the user audit records.		
8.	The System Admin with sufficient privileges shall only restore the user access further to failed attempts, and shall not automatically allow access.		
9.	The System Authorization service shall control the access limits of the respective logged in users. Authorization shall validate an authenticated user's request and grant/deny him permission to perform a requested operation.		
10.	The System Authorization level shall be extensible towards a fine gained security wherein the users shall perform the operations based on the data like location or department.		
	User Administration		
1.	The System shall provide a Super User who shall administrate the system User Groups and its privileges. Super User shall be the system Security Administrator (System Admin).		
2.	The system shall have role based access.		
3.	The System Admin shall create User Groups as per the profiles with pre-defined privileges.		
4.	The System Admin shall be able to administer user / password of users across all groups and privileges across all user groups.		
5.	The System Admin shall have the rights to create users and administer username/password of User Group / Users. Users created shall derive its default privileges as per the User Group created by System Admin.		

Make: **Model:**			
S.No.	**Functionality**	**Compliance (Y/N)**	**Remark (If any)**
6.	The System shall support users belonging to multiple groups.		
7.	The System shall be customizable towards multitenant architecture that allows distributing the secured user administration to select group(s) to administer users within their organization. The System shall support auto generation of password.		
8.	The System shall be customizable towards Two Factor Authentication with OTP (One Time Password) support.		
9.	The System shall send mail notification on key admin transactions like account creation along with first time password		
	User Audit		
1.	The System shall provide facility to audit the authentication and authorization related information and stored in.		
2.	Auditing shall monitor the selected operations performed by the user.		
3.	The User Audit trails shall be logged and viewed by authorized security admin, it includes views of the current users logged in and past users logged in/out and the operations performed.		
4.	All authorized operations that are performed are audited and logged in the audit tables.		
5.	Any erroneous and suspicious activities like login attempt failures shall be logged and viewed part of audit.		
6.	The system shall provide audit reports on the performed operations with it user information and time stamps.		
	Warranty Support		
7.	Comprehensive OEM Support for 5 Years		

11.3.5. Backup Software

S. No.	Specifications	Compliance (Yes / No)	Deviation (if any)
1.	Proposed Backup software should be in Gartner's leader quadrant for last three years in Gartner Magic Quadrant report for Data Protection / Backup Software.		
2.	The proposed Backup software must offer suitable licenses (host-based or capacity-based) with no restrictions on type of arrays and front-end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied as part of proposed solution.		
3.	Licenses supplied should have licenses for Backup and Replication workloads.		
4.	Backup software should have Capability to do trend analysis for capacity planning of backup environment, extensive alerting, and reporting. Any specialized modules and resources needed must be quoted along with Backup solution to achieve this functionality.		
5.	Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance, and workload of the virtual hosts.		
6.	Proposed solution should support automated action for popular alarms (automated or semi-automated), with at-a-glance and drill-down views of health, performance, and workload of the virtual hosts.		
7.	Backup software should support agentless backups of applications residing in VMs like SQL, Exchange, SharePoint, Oracle, etc. with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads.		
8.	Backup software should support multi–OEM Hardware and Software and it should support snapshot integration with hypervisors like VMware, Hyper-V, RedHat, Xen, Acropolish, etc. and support de-duplication (at source level and at data travel) on any storage target. It should be able to backup data to tapes (like LTO) as well for long term retention.		
9.	Backup software should support file level recovery from any backup of any VM or physical server. It should support a full system recovery in case of a system crash, either on a physical system or virtual machine.		
10.	Backup software should have integrated data de-duplication engine with multi-vendor storage support to save space by storing de-duplicated copies of data. The de-duplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be		

S. No.	Specifications	Compliance (Yes / No)	Deviation (if any)
	supplied along with other components		
11.	Backup software should provide Backup and Replication capabilities in one console only and allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only those VMs to which they have access, without administrator intervention, thereby delivering self-serve capabilities.		
12.	The proposed Backup software must Support Seamless Integration with Point-in-time storage snapshots in the environment to perform faster LAN Free backup without any overhead to Hypervisor Compute Layer, allowing recovery at the application level, the file level, and the VM level.		
13.	Backup software should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup within 15 Minutes RTO.		
14.	The Proposed solution should support Continuous replication at VM level. The RPO must be less than 5-15 Seconds and it must deliver Application consistency.		
15.	The proposed solution should be able to publish Disaster recovery plans and update them through automated discovery whenever prompted after changes in infrastructure.		
16.	Proposed disk based backup appliance should be able to interface with various industry leading server platforms, operating systems and Must support LAN and SAN based D2D backup and VTL backup simultaneously.		
17.	**Support & Warranty** Support / warranty documents for five Years from the OEM should be submitted		

11.3.6. Backup Appliance

S/N	Specification	Compliance (Yes / No)	Remark (if Any)
Make : **Model :**			
	General Specification for Disk based Backup Appliance		
1	Proposed disk based backup appliance must be a physical appliance and should be able to interface with various industry leading server platforms, operating systems. It Must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS v3, CIFS, FC , OST and NDMP protocols.		
2	Proposed appliance should support global and inline data duplication using automated variable block length deduplication technology.		
3	Proposed appliance should have the ability to perform different backup, restore, replication jobs simultaneously and Must supports communications and data transfers through 8GB SAN, 10 Gb & 1 Gb Ethernet LAN over copper and SFP+. The proposed backup appliance should be offered with min. 2 x 1Gbps NIC, 4 x 10Gbps NIC and 2 x 16Gbps FC ports		
4	Proposed appliance should support minimum backup throughput of 7 TB/hr while maintaining a single deduplication pool with RAID 6 and min. one hot spare disk as well. The disks used should be of 3TB / 4TB in size with the ratio of 15:1 or better		
5	Proposed appliance should support bi-directional, many-to-one, one- to-many, and one-to-one replication		
6	Proposed appliance should support 256 bit AES encryption for data at rest and data-in-flight during replication. It should offer internal and external key management for encryption		
7	The proposed disk appliance must be configured with 16 TB of usable disk capacity (i.e. post RAID 6, hot spare, overheads, etc.). It must be support a minimum of 2X scalability i.e. 32 TB or higher in the same appliance.		
8	Warranty: 5 Years 24 X 7 Support with NBD Part Replacement comprehensive warranty.		

11.3.7. DESKTOP

Make: **Model:**				
SL	**Parameter**	**Functionality**	**Compliance (Y/N)**	**Remark (If Any)**
1	Processor	Intel 12th Generation Core i7-12700 CPU or better		
2	Chipset	Suitable OEM chipset		
3	Motherboard	OEM Motherboard		
4	Memory	16GB DDR4 expandable to 32GB DDR4, Total four DIMM slots		
5	Hard Disk Drive	1 TB 7200 RPM SATA Hard Drive		
		500 GB NVME M2 SSD PCIE 3.0 x4		
6	Graphics	Intel HD Graphics (integrated)		
7	Audio	High Definition Audio (all ports are stereo), with Internal Speaker		
8	Ethernet	Integrated Gigabit (10/100/1000 NIC) LAN		
9	Slots	All FULL height Slots		
		(1) PCI Express x16		
		(1) PCI Express x1		
		(1) PCI x1		
10	Bays	(1) 3.5” Internal drive bays		
		(1) 5.25" ODD		
11	Ports	At least 8 USB ports with minimum 4 x USB 3.0 ports and 4 x USB 2.0 ports with at least 2 on the front side		
		PS/2 keyboard and mouse ports		
		(1) VGA video port / HDMI port		
		(1) RJ-45 network connector		
		Rear Line In/Line Out jacks		
		Front 3.5mm headphone output and microphone in jack		
12	Form Factor	MT (Micro Tower)		
13	Power Supply	240 to 300W Active PFC, 85% efficient Power supply		
14	Keyboard	PS2/USB 104 keys keyboard (Same make as PC)		
15	Mouse	PS2/USB 2 Button Scroll Mouse (Same make as PC)		
16	Security	TPM 1.2 Security Chip		
		SATA port disablement (via BIOS)		
		Optional USB Port Disable at factory (user configurable via BIOS)		
		Removable media write/boot control		

Make: Model:				
SL	**Parameter**	**Functionality**	**Compliance (Y/N)**	**Remark (If Any)**
		Power-On password (via BIOS)		
		Administrator password (via BIOS)		
		Setup password (via BIOS)		
		Support for chassis padlocks and cable lock devices		
17	Operating System	Preinstalled Genuine Microsoft Windows10Pro(64-bit) with License and Recovery CD or latest version		
18	Software	Preloaded Genuine Microsoft Office (Latest Version) & Anti-Virus		
19	Compliance and Certification	ROHS and Win certification		
		Energy Star ver 5.2		
		EPEAT certified for India		
20	Monitor	21" Wide TFT TCO Certified with matching port of workstation/desktop		
20	Warranty	5 years OEM Onsite warranty		

11.3.8. Multifunction Network Printer

Make: Model:				
SL	**Parameter**	**Functionality**	**Compliance (Y/N)**	**Remark (If Any)**
1	Type	Monochrome		
2	Functions	'3-in 1' (Print, Copy, Scan)		
3	Print Speed (Monochrome) (A4)	27ppm or Higher		
4	Print Resolution	600 x 600dpi or Higher		
5	Copy Speed (A4)	27 cpm		
6	Copy Resolution	600 x 600dpi or Higher		
7	Scan Speed	Minimum 3.0 sec per sheet (mono) Minimum 4.0 sec per sheet (colour)		
8	Optical Scan Resolution	600 x 600dpi or Higher		
9	Auto Duplex Printing	Yes		
10	Auto Document Feeder (ADF)	Yes		
11	Interface	High-Speed USB 2.0		
		10 / 100 Base-T Ethernet		

Make: Model:				
SL	**Parameter**	**Functionality**	**Compliance (Y/N)**	**Remark (If Any)**
		Wi-Fi 802.11b/g/n (Infrastructure mode, WPS Easy Setup, Direct Connection)		
12	Network Support	IPv4 & IPv6		
13	Power Consumption	1 150W or less		
14	Operating Environment	Temperature: 10 - 30°C Humidity: 20 - 80% RH (no condensation)		
15	Operational Panel	LCD		
16	Warranty	5 Years OEM Warranty		

11.3.9. SAN Switch

Make: Model:			
SL	**Functionality**	**Compliance (Y/N)**	**Remark (If Any)**
1.	Minimum Two no's of SAN switches to be offered. Each fibre switch should be quoted with minimum 48 active FC ports modules of 32Gbps speed each with necessary Licenses.		
2.	Each SAN switch needs to be configured and supplied with Short range transceiver modules.		
3.	The switch should have support for 8/16/32 Gbps HBA.		
4.	The switch should have auto sensing, Zoning, Ethernet and Serial Port for communication		
5.	Switch should be rack mountable 1U size and should be supplied with mounting kit.		
6.	The switch should be equipped with redundant hot swap power supply and allow hot swap ability without resetting the switch, or affecting the operations of the switch		
7.	The switch should be backward compatible		
8.	The switch should be capable for non-disruptive firmware update		
9.	The switch should be capable of End-to-end performance monitoring		
10.	The switch should have Support for POST & online diagnostics		
11.	The switch should be capable to interface with host-based adapters (HBA) of multiple OEM,		

Make: **Model:**			
SL	**Functionality**	**Compliance (Y/N)**	**Remark (If Any)**
	supporting multiple Operating Systems		
12.	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs)/Virtual Fabric, Port Zoning and LUN Zoning		
13.	The switch should support IPv6 from day one		
14.	Switch must support out-band management protocols like SNMP v3, SMI-S, Telnet & TFTP/SFTP		
15.	The switch should have following Zoning and security features:		
16.	a. Support for hardware -enforced zoning		
17.	b. Policy based security and centralized fabric management		
18.	c. Support for secure access		
19.	d. Support for FC based authentication		
20.	e. Support for TACACS+ or RADIUS, SSH, SNMP		
21.	f. Support for port binding		
22.	g. Support for Hardware based Inter Switch linking / Trunking		
23.	h. Support for dynamic Load balancing of links with no overhead		
24.	All relevant licenses for above features should be quoted along with switch		
25.	OEM must have India presence for last 5years on both Sales and Support operation		
26.	Offered SAN switches will be integrated to the existing SAN fabric deployment on HPE B-series SAN switches. Required licensing and services to be included in the offer.		
27.	Comprehensive OEM Warranty for 5 Years		

11.3.10. Server

Make: **Model:**				
Sl. No.	**Minimum Requirement Specification**		**Compliance (Y/N)**	**Remarks**
1	Processor	The server should have 2 nos. of Intel Xeon/AMD latest Generation Processor: 2 x 32 cores, minimum 2.8 GHz clock rate. 64-bit x86 processor fully binary compatible to 64/32-bit applications. Number of cores on a single die/socket		

Make: **Model:**				
Sl. No.	**Minimum Requirement Specification**		**Compliance (Y/N)**	**Remarks**
		will be treated as a single processor		
2	Memory	1 TB latest DDR memory using 64 GB DIMM's or higher. Advanced ECC with multi-bit error protection. The proposed expandability should be met by adding more memory modules of same/higher capacity		
3	HDD Controller	12 Gbps SAS RAID Controller supporting RAID 0, 1, 5 and 6 with 2GB battery backed up Cache		
4	HDD	4 x 300 GB SSD or higher		
5	Video Controller	Integrated Graphics Controller		
6	Network Controller	Minimum 2 x 1 Gbps copper/BaseT ports & Two no's Dual 10/25 Gbps SFP25 (25G-SR populated) ports with four no's of 5mtr of FC cable.		
7	Fiber Channel HBA	Two no's Dual FC Port 32 Gbps with four no's of 5mtr LC-LC Cable		
8	Slots	Minimum one free PCI/PCI-x/PCI-Express 4.0		
9	Ports	2* USB; One dedicated Ethernet Port for OS independent out-of-band hardware management		
10	Bays	Minimum 8 Hot Swap drive bays		
11	Optical Drive	DVD ROM Internal/External		
12	System Chassis	Rack Mount, 2U (max), Redundant Hot Swappable Power Supply with platinum efficiency		
13	OS certification	Certification for latest Server version of Windows and minimum two Linux flavors		
14	Drive/Software utilities	All required device drivers for OS installation, System Configuration and Server Management		
15	System Management	• Monitoring ongoing management, service alerting, reporting and remote management with embedded dedicated Gigabit out of band management port. Remote Management of Server over LAN & WAN with SSL encryption, Virtual Media and virtual folder with required advanced license, Remote KVM, Server		

Make: **Model:**				
Sl. No.	**Minimum Requirement Specification**		**Compliance (Y/N)**	**Remarks**
		Health logging, Directory Services compliance (AD or LDAP), Multi-factor authentication, REST/XML API, group management of power, configuration, licenses including firmware, Configuration backup, Syslog (local & remote).		
		• Management software should support integration with popular virtualization platform management software like vCentre, SCVMM and Red Hat RHEV.		
		• Offered Server platform must be ready for container workload deployment		
16	Serviceability	• System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone support. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur. Should provide remote firmware update functionality.		
		• Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD. Solution should help simplify the infrastructure management plan.		
		• Solution should be provided for monitoring & analysis feature to predict, prevent and auto-resolve problems and by providing automating case creation and log file submission for the problems that can't be auto-resolved. Solution shall help simplify the infrastructure management plan. Should provide silicon-based hardware root of trust, automatic secure BIOS recovery, cryptographically signed firmware updates		
17	Virtualization	Should support Industry Standard Virtualization Software		
18	IDC Ranking	OEM should be ranked within Top 5 as per published IDC report for Server in		

Make: **Model:**				
Sl. No.	**Minimum Requirement Specification**		**Compliance (Y/N)**	**Remarks**
		India during any of last four quarters Letter/report from IDC should be attached along with the bid.		
19	Warranty	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support		
20	IPv6 support	All devices should be IPv6 implementation ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation		
21	OEM Criteria	a) Server OEM shall be in the leader's quadrant of the latest published Gartner's MQ report on Modular Servers b) OEM must have India presence for last 5 years on both Sales and support operation.		

11.3.11. STORAGE

Make: **Model:**				
Sl.No	**Description**	**Minimum specification**	**Compliance (Y/N)**	**Remark (If any)**
1	Controllers	System should be an unified storage to support both file and block without adding any additional hardware. The Block services should not be SAN emulated on File System. System should be configured with Dual controllers. There should be a single GUI for management of both file and block services. The controllers should be active- active.		
2	Controller Operating System Support	The NAS operating system of the vendor should be based on Unix or Linux based operating system, incase if it is a modified Unix or Linux OS for should be a NAS		

Make: **Model:**				
Sl.No	**Description**	**Minimum specification**	**Compliance (Y/N)**	**Remark (If any)**
		operations optimized OS		
3	Cache	The system should have a minimum of 128 GB of cache/ system memory across dual controllers. The cache should be persistent across all controllers offered. Data in the cache should be protected from unlimited period of power outage. Additionally, the same storage should support SSD / Flash as extended Read and Write Cache which can be added in future in the same storage system. If extended cache is not able to do write caching, then equivalent capacity of memory (DRAM) should be provided for write caching.		
4	Disk Support	System should support drive type of SSD drives, SAS 12 Gb/s and SATA II 7200 RPM/Nearline SAS 7200 RPM drives. Storage should be provided with File level retention and 256 Bit encryption (FIPS 140-2 compliant) to be offered from Day 1.		
5	Protocols and Ports Support	CIFS, NFS, FC, iSCSI (1 and 10 Gb) support required. The system is to be configured with 8 x 16Gbps FC ports and 8 nos of 10Gbps iSCSI / IP ports.		
6	Other Protocols Support	The System should support SNMP, Address resolution protocol, Simple Network Time Protocol, LDAP, Network Lock Manager v4.		
7	Software licenses	The system should be configured with licenses for FC and iSCSI. CIFS, NFS. Thin Provisioning, Virtualization integration software license should be provided for		

Make: **Model:**				
Sl.No	**Description**	**Minimum specification**	**Compliance (Y/N)**	**Remark (If any)**
		entire system.		
8	Performance Monitoring Software	Performance Monitoring and reporting software should be provided. This should provide details of performance like IOPs, utilization, response time and provide capacity details like amount of capacity allocated, capacity used and capacity free.		
9	Snapshots	The system should be configured with Snapshot licenses, snapshot restore licenses for the entire systems capacity.		
10	RAID Support	Should support RAID 10, 5 and 6.		
11	Management	Support a browser based built in management. Should be able to support automated email to vendor support center for proactive maintenance. There should be a dedicated Ethernet port for management and it should not use the iSCSI host ports for management.		
12	Storage space	The bidder should configure Storage system with 20TB usable capacity using SAS 10K drives in RAID 5. The storage should scalable upto 100TB.		
13	Automated Tiering	Storage array be configured with license automated tiering at Sub-LUN level across all the 3 tiers of storage, i.e., EFD, SAS and NL-SAS. It should support simultaneous movement of Sub-LUN data from NL- SAS to SAS to EFD and vice versa based on application I/O workload.		

Make: **Model:**				
Sl.No	**Description**	**Minimum specification**	**Compliance (Y/N)**	**Remark (If any)**
14	Replication	Storage array should be configured with license for Replication.		
15	Warranty and Support	5 Years Support with parts Replacement.		

12. Annexure- 1: Particulars of the Bidders

Sl. No.	Information Sought	Details to be Furnished
1	Name of the bidding Company	
2	Address of the Company	
3	Incorporation status of the firm (Public limited / Private limited, etc.)	
4	Year of Establishment	
5	Date of registration	
6	RoC Reference No.	
7	Details of company registration	
8	Details of registration with appropriate authorities for GST	
9	Name, Address, e-mail ID, Phone nos. and Mobile Number of Contact Person	
10	Roles & Responsibilities	

Name of the Bidder: .....
Authorized Signatory: .....
Signature:
Seal:
Date:
Place:

13. Annexure-2: Bidder's Authorization Certificate

(To be filled by the Bidder)

To,

The General Manager (Admn.)
Odisha Computer Application Centre (OCAC)
OCAC Building, Plot No.-N-1/7-D, Acharya Vihar Square, RRL
Post Office, Bhubaneswar-751013 (INDIA)

I/ We {Name/ Designation} hereby declare/ certify that {Name/ Designation} is hereby authorized to sign relevant documents on behalf of the company/ firm in dealing with RFP reference No. OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022. He/ She is also authorized to attend meetings & submit technical & commercial information/ clarifications as may be required by you in the course of processing the Bid. For the purpose of validation, his/ her verified signatures are as under.

Thanking you,

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

14. Annexure-3: Bid Security Declaration

(To be submitted on the Letterhead of Bidder)

To
The General Manager (Admin),
Odisha Computer Application Centre,
N-1/7-D, Acharya Vihar P.O. RRL,
Bhubaneswar - 751013.

Subject: Bid Security of RFP for Selection of Agency for Implementation, Operations and Maintenance of OSWAN NOC

Ref: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022

Madam,

I/We understand that, as per clause no. _____above referenced RFP, bids must be supported by a Bid Security Declaration In lieu of Earnest Money Deposit, (*reference Finance Department, Government of Odisha, Office Memorandum No. 281/F, dated 05.01.2022*). I/We hereby accept that, I/We may be disqualified from bidding for any contract with you for a period of three years from the date of disqualification as may be notified by you (without prejudice to OCAC's rights to claim damages or any other legal recourse) if,

1) I am /We are in a breach of any of the obligations under the bid conditions,
2) I/We have withdrawn or unilaterally modified/amended/revised, my/our Bid during the bid validity period specified in the form of Bid or extended period, if any.
3) On acceptance of our bid by OCAC, I/we failed to deposit the prescribed Security Deposit or fails to execute the agreement or fails to commence the execution of the work in accordance with the terms and conditions and within the specified time.

Yours faithfully,

Authorized Signatory with Date and Seal:
Name:
Title:
Address of Bidder:

15. Annexure-4: RFP Form

(To be filled by the Bidder)

1) **Addressed to:**

Name of the Tendering Authority	The General Manager (Admin.)
Address	Odisha Computer Application Centre (OCAC) OCAC Building, Plot No.-N-1/7-D, Acharya Vihar Square, RRL Post Office, Bhubaneswar-751013 (INDIA)
Telephone	0674-2567280 / 2567064 /2567295 / 2588283
Tele Fax	0674-2567842
Email	gm_ocac@ocac.in

2) **Firm Details:**

Name of Firm				
Name of CMD of the firm with email id, contact number				
Name of Contact Person with Designation				
Registered Office Address				
Address of the Firm				
Year of Establishment				
Type of Firm Put Tick (√) mark	Public Limited	Private Limited	Partnership	Proprietorship
Telephone Number(s)				
Email Address/ Web Site	Email:		Web-Site:	
Fax No.				
Mobile Number	Mobile:			
Certification/Accreditation/Affiliation, if Any				

3)The requisite tender fee amounting to Rs. _____/- (Rupees <in words>) has been deposited vide DD/BC/receipt no. _____ dated _____.

4) The requisite EMD amounting to toRs. _____/- (Rupees <in words>) has been deposited vide Bank Guarantee / DD No. _____ dated _____.

5) We agree to abide by all the terms and conditions mentioned in this form issued by the Empanelment Authority and also the further conditions of the said notice given in the attached sheets (all the pages of which have been signed by us in token of acceptance of the terms mentioned therein along with stamp of the firm).

Date:

Name & Seal of the firm: _____

Authorized Signatory: _____

16. Annexure-5: Covering Letter - Technical Bid

(To be filled by the bidder and signed in Company Letter Head)

To
The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of I.T. Dep't, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL,
Bhubaneswar - 751013

Subject: Technical Proposal for Selection of Agency for Implementation, Operations and Maintenance of OSWAN NOC vide RFP Ref.No. OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022.

Sir/Madam,

We, the undersigned, offer to provide our services against your RFP enquiry no. <*Insert RFP no*> dated <*insert date*>. We are hereby submitting our Proposal, which includes this Technical Bid sealed in the envelope.

We hereby declare that all the information and statements made in this Technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification.

We agree to abide by all the terms and conditions of the tender document. We would hold the terms of our bid valid for 180 days as stipulated in the RFP document.

We agree that you are not bound to accept the lowest or any bid response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products / services specified in the bid response without assigning any reason whatsoever.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company /firm/organization and empowered to sign this document as well as such other documents which may be required in this connection.

Yours sincerely,
Authorized Signature [*In full and initials*]: _____
Name and Title of Signatory: _____
Name of Firm: _____
Address: _____

17. Annexure-6: Manufacturer's Authorization Form (MAF)

(To be submitted in OEM Letterhead)

Letter No._____ Date: _____

To
The General Manager (Admin)
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
P.O.- RRL, Bhubaneswar – 751013

Sub: OEM Authorization Letter

RFP Ref No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022

Dear Sir

We, who are established and reputable manufacturers / producers of _____ having factories / development facilities at (*address of factory / facility)* do hereby authorize M/s _____ *(Name and address of Agent)* to submit a Bid, and accept the Purchase Order against the above Bid Invitation.

We hereby extend our full guarantee and support for the Solution, Products and services offered by the above firm against this Bid Invitation.

SUPPORT AND MAINTENANCE: In the event that, during the contract term specified in the RFP, _____ (Bidder Name)is unwilling or unable to fulfil its maintenance and support in respect of the Hardware or Software products in accordance with the RFP, _____ (OEM Name) undertakes to provide such support and maintenance obligations (either by ourselves or through a subcontractor) in accordance with the RFP Technical Terms of Service for the duration of any paid up Support and Maintenance Term provided always that you have a valid Subscription Agreement.

We duly authorize the said firm to act on our behalf in fulfilling all installations, Technical support and maintenance obligations required by the Project.

Yours faithfully,

(Name)

Seal

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its bid.

18. Annexure-7: Financial Bid Cover Letter and Format

(To be filled by the bidder and signed in Company Letter Head)

Location:
Date:

To

The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of I.T. Dep't, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL,
Bhubaneswar – 751013

Subject: Submission of the financial bid for Selection of Agency for Selection of Agency for Implementation, Operations and Maintenance of OSWAN NOC .

RFP Ref No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022.

Dear Sir/Madam,

We, the undersigned, offer to provide the services in accordance with your Request for Proposal cited above and our Proposal (Technical and Financial Proposals). Our attached Financial Proposal is for the sum of [*Amount in words and figures*] for 5 Years support & update. This amount is inclusive of the local taxes.

1. Price and Validity

All the prices mentioned in our RFP are in accordance with the terms as specified in the RFP documents. We declare that our Bid Price is for the entire scope of the work as specified in the appropriate section in the RFP. All the prices and other terms and conditions of this Bid are valid minimum for a period 180 days from the date of opening of the Bid. However, we also confirm that our price bid will remain valid for 1 years from the opening date, if selected.

We hereby confirm that our prices do not include any taxes and duties.

We understand that the actual payment would be made as per the existing tax rates during the time of payment.

2. Unit Rates

We have indicated in the relevant forms enclosed, the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

3. Qualifying Data

We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our bid, we agree to furnish the same in time to your satisfaction.

4. Bid Price

We declare that our Bid Price is for the entire scope of the work as specified in the RFP. These prices are indicated at Price Bid attached with our bid as part of the Bid.

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

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

We understand that our bid is binding on us and that you are not bound to accept a bid you receive.

Thanking you,
We remain,

Yours sincerely,

Authorized Signature:

Name and Title of Signatory:

Name of Firm:

Address:

19. Annexure-8: Financial Capabilities

(To be filled by the Bidder)

Turnover (Rs. In Crores)		
2016-2017	**2017-2018**	**2018-2019**
Net worth (Rs. In Crore)		
2016-2017	**2017-2018**	**2018-2019**

Name of the Bidder: .....
Authorized Signatory: .....
Signature:
Seal:
Date:
Place:

20. Annexure-9: Self-Declaration

(Non-blacklisted in company Letter Head)

To
The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of I.T. Dep't, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL,
Bhubaneswar - 751013

Sir
In response to the RFP Ref. No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022 for RFP titled "_____", as an owner/ partner/ Director of (organization name) _____ I/ We hereby declare that presently our Company/ firm is not under declaration of ineligible for corrupt & fraudulent practices, blacklisted either indefinitely or for a particular period of time, or had work withdrawn, by any State/ Central government/ PSU.

I/We further declare that there is no past / ongoing legal trial in name of any of the Owner / Partner / Director of the bidding company as on the tender submission date.

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

Thanking you,
Name of the Bidder: .....
Authorized Signatory: .....
Signature:
Seal:
Date:
Place:

21. Annexure-10: Project Citation Format

(To be filled by the Bidder)

Relevant IT Project Experience	
General Information	
Name of the project	
Client for which the project was executed	
Name and contact details of the client	
Project Details	
Description of the project	
Scope of services	
Other Details	
Total cost of the project	
Duration of the project (no. of months, start date, completion date, current status)	

Name of the Bidder: .....
Authorized Signatory: .....
Signature:
Seal:
Date:
Place:

22. Annexure-11: Detailed Bill of Material

To be submitted by Bidder in their Letter Head

Sl No	OSWAN-NOC Components	Unit	Qty	Make	Model
IT Infrastructure					
1					
2					
3					
4					
Non- IT Infrastructure					
1					
2					
3					
4					
5					

Name of the Bidder: .....
Authorized Signatory: .....
Signature:
Seal:
Date:
Place:

BLANK PAGE

23. Annexure-12: PRICE BID FORMAT

Bidder will submit the Price Bid as per the BoQ in Annexure-11

RFP Enquiry No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022					
RFP for selection of agency for Implementation, Operations and Maintenance of OSWAN NOC					
Annexure-12.1 Abstract of Cost Components					
#	**ITEM**	**COST (INR)**	**TAX (INR)**	**Total Tax (INR)**	**TOTAL PRICE including Tax (INR)**
1.	CAPEX (C)				
2.	OPEX for 5 Years (O)				
3.	Manpower (M)				
4.	INPLIMENTATION COST (I)				
5.	Any Other Cost (If Any)				
TOTAL (C+O+M+I):					
TOTAL IN WORDS:					

RFP Enquiry No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022								
RFP for selection of agency for Implementation, Operations and Maintenance of OSWAN NOC								
Annexure-12.2 CAPEX (C)								
#	**OSWAN-NOC Components**	**Unit**	**Qty**	**Unit Price in INR**	**Total Cost (INR)**	**Tax (%)**	**Total Tax (INR)**	**Total Cost including Tax (INR)**
IT Infrastructure (CA)								
1.	Rack Mount Server	No's	5					
2.	SAN Storage – 20 TB usable and scalable upto 100TB	No's	1					
3.	SAN Switch - 24 ports scalable up to 48 ports	No's	2					
4.	DMZ Switch	No's	2					
5.	24 port L3 Network Switch	No's	2					
6.	Access PoE Switch	No's	4					
7.	**NMS, Automation & Helpdesk Management System for OSWAN Equipment**	Set	1					
a.	IT Network Discovery & Monitoring	Set	1					
b.	NMS Server Infrastructure Monitoring	Set	1					
c.	IT Network Fault Management	Set	1					
d.	IT Performance Management	Set	1					
e.	IT Service Management	Set	1					
f.	IT Network Performance Management	Set	1					
g.	Reporting and Dashboards	Set	1					
h.	Automation	Set	1					
i.	User Interface, User Authentication & Authorization, User Administration & User Audit	Set	1					
8.	Backup Software	Set	1					
9.	Backup Appliance with 16 TB usable capacity	Set	1					
10.	Virtualisation Software	As Required	10					
11.	One time implementation and upgradation cost of existing setup	Set	-					
12.	Windows Server OS Standard Edition (Latest	As Required						

RFP Enquiry No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022								
RFP for selection of agency for Implementation, Operations and Maintenance of OSWAN NOC								
Annexure-12.2 CAPEX (C)								
#	**OSWAN-NOC Components**	**Unit**	**Qty**	**Unit Price in INR**	**Total Cost (INR)**	**Tax (%)**	**Total Tax (INR)**	**Total Cost including Tax (INR)**
	version) as per Bidder's solution							
13.	Linux Server OS Enterprise Edition (Latest version) as per Bidder's solution	As Required						
14.	Enterprise Analytical Database as per Bidder's solution	As Required						
15.	Server Security solution (HIPS) Licences, as per Bidder's solution	As Required						
16.	Desktop with Preloaded Windows & MS Office, Antivirus	No's	3					
17.	Multifunctional Printer	No's	1					
18.	Any Other IT components (please specify)							
Non-IT Infrastructure (CB)								
1.	Civil & Interior Works (Including Dismantling & Construction of Brick work, masonry work, painting, Partition, False floor, Raised Floor, False ceiling, Water proofing, etc.	Set	1					
2.	Electrical System Works (Including electrical panel, Earthing, NOC internal electrical wiring, DB, Switchgears, Lighting & fixtures, etc for all NOC Areas, DC Areas, Helpdesk Areas & Office Areas)	Set	1					
3.	40 KVA Modular UPS with VRLA battery for minimum 30 Min Backup on full load for the Server Farm Area and Helpdesk areas.	No's	2					
4.	Precision Air Conditioning System for the Server Farm Area	No's	4					
5.	Comfort Air Conditioning for the Helpdesk Areas & Office Areas	Set	1					

RFP Enquiry No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022								
RFP for selection of agency for Implementation, Operations and Maintenance of OSWAN NOC								
Annexure-12.2 CAPEX (C)								
#	**OSWAN-NOC Components**	**Unit**	**Qty**	**Unit Price in INR**	**Total Cost (INR)**	**Tax (%)**	**Total Tax (INR)**	**Total Cost including Tax (INR)**
6.	Fire Suppression and Detection System (for all Areas)	Set	1					
7.	VESDA System	Set	1					
8.	Water Leak Detection System	Set	1					
9.	Access Control System	Set	1					
10.	IP CCTV System	Set	1					
11.	Public Address System	Set	1					
12.	Rodent Repellent System	Set	1					
13.	Fire extinguisher	Set	1					
14.	Building Management Solution	Set	1					
15.	Video Wall (3x2) with Controller and accessories	Set	2					
16.	Intelligent Racks	No's	12					
17.	Passive Networking (including Cat-6 Cable, Patch panel, MPO cassettes, Cable basket, Fibre Runner, I/O module, Patch Cord-Copper/Fiber, Faceplate, Wall mount Rack, Conduit with accessories)	Set	1					
18.	IP KVM switch	Set	1					
19.	Any Other IT components (please specify)							
				Total				
Total in words:								

RFP Enquiry No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022								
RFP for selection of agency for Implementation, Operations and Maintenance of OSWAN NOC								
Annexure-12.2 OPEX (O)								
#	**OSWAN-NOC Components**	**Unit**	**Qty**	**Unit Price for 5 years warranty/ support in INR**	**Total Cost (INR)**	**Tax (%)**	**Total Tax (INR)**	**Total Cost including Tax (INR)**
IT Infrastructure (CA)								
1.	Rack Mount Server	No's	5					
2.	SAN Storage – 20 TB usable and scalable upto 100TB	No's	1					
3.	SAN Switch - 24 ports scalable up to 48 ports	No's	2					
4.	DMZ Switch	No's	2					
5.	24 port L3 Network Switch	No's	2					
6.	Access PoE Switch	No's	4					
7.	**NMS, Automation & Helpdesk Management System for OSWAN Equipment**	Set	1					
a.	IT Network Discovery & Monitoring	Set	1					
b.	NMS Server Infrastructure Monitoring	Set	1					
c.	IT Network Fault Management	Set	1					
d.	IT Performance Management	Set	1					
e.	IT Service Management	Set	1					
f.	IT Network Performance Management	Set	1					
g.	Reporting and Dashboards	Set	1					
h.	Automation	Set	1					
i.	User Interface, User Authentication & Authorization, User Administration & User Audit	Set	1					
8.	Backup Software	Set	1					
9.	Backup Appliance with 16 TB usable capacity	Set	1					
10.	Virtualisation Software	As Required	10					
11.	One time implementation and upgradation cost of existing setup	Set	-					
12.	Windows Server OS Standard Edition (Latest version) as per Bidder's solution	As Required						

13.	Linux Server OS Enterprise Edition (Latest version) as per Bidder's solution	As Required						
14.	Enterprise Analytical Database as per Bidder's solution	As Required						
15.	Server Security solution (HIPS) Licences, as per Bidder's solution	As Required						
16.	Desktop with Preloaded Windows & MS Office, Antivirus	No's	3					
17.	Multifunctional Printer	No's	1					
18.	Any Other IT components (please specify)							
Non-IT Infrastructure (CB)								
1.	Civil & Interior Works (Including Dismantling & Construction of Brick work, masonry work, painting, Partition, False floor, Raised Floor, False ceiling, Water proofing, etc.	Set	1					
2.	Electrical System Works (Including electrical panel, Earthing, NOC internal electrical wiring, DB, Switchgears, Lighting & fixtures, etc for all NOC Areas, DC Areas, Helpdesk Areas & Office Areas)	Set	1					
3.	40 KVA Modular UPS with VRLA battery for minimum 30 Min Backup on full load for the Server Farm Area and Helpdesk areas.	No's	2					
4.	Precision Air Conditioning System for the Server Farm Area	No's	4					
5.	Comfort Air Conditioning for the Helpdesk Areas & Office Areas	Set	1					
6.	Fire Suppression and Detection System (for all Areas)	Set	1					
7.	VESDA System	Set	1					
8.	Water Leak Detection System	Set	1					
9.	Access Control System	Set	1					
10.	IP CCTV System	Set	1					
11.	Public Address System	Set	1					
12.	Rodent Repellent System	Set	1					
13.	Fire extinguisher	Set	1					
14.	Building Management Solution	Set	1					
15.	Video Wall (3x2) with Controller and accessories	Set	2					
16.	Intelligent Racks	No's	12					
17.	Passive Networking (including Cat-6 Cable, Patch panel, MPO cassettes, Cable basket, Fibre Runner, I/O module, Patch Cord-	Set	1					

	Copper/Fiber, Faceplate, Wall mount Rack, Conduit with accessories)							
18.	IP KVM switch	Set	1					
19.	Any Other IT components (please specify)							
					Total			
Total in words:								

RFP Enquiry No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022												
RFP for selection of agency for Implementation, Operations and Maintenance of OSWAN NOC												
Manpower Cost in INR (M)												
#	**Resource**	**Unit**	**Qty**	**Cost Per Resource (1st Year)**	**Cost Per Resource (2nd Year)**	**Cost Per Resource (3rd Year)**	**Cost Per Resource (4th Year)**	**Cost Per Resource (5th Year)**	**Total Resource Cost for Total 5Year**	**Tax (%)**	**Total Tax (INR)**	**Total Cost including Tax (INR)**
1	NMS Specialist	No's	1									
2	BMS Specialist	No's	1									
3	Electrical Assitant	No's	3									
									TOTAL			
Total in Words :												

Note: The bidder as applicable will install all above-mentioned components. Bidder are requested to visit the site before they propose their solution and estimate the amount of work as per the area allocated. The unit rates of each elements must be mentioned separately and if more quantity will be ordered by the later stage, the payment will be made on actual basis. The specification mentioned for components are minimum, bidders are free to provide any item/s meeting the minimum requirements.

Blank Page

24. Annexure-13: Pre-Bid Query Format

PRE-BID QUERIES FORMAT					
RFP ENQ. No.- OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022					
Request for Proposal (RFP) :					
Name of the Company/Firm:					
Bidding document Fee Receipt No._____/ DD No._____ Dated:_____ for Rs. _____					
Name of the Person(s) Representing the Company/Firm:					
Name of Person		**Designation**		**Email ID(s)**	**Tel. Nos. & Fax Nos.**
S.No.	**Page No.**	**Clause No**	**RFP Clause**	**Query /Clarification**	**Suggestion if any**

25. Annexure-14: Details of documents to be submitted by the bidder

Sl. No.	Documents to be submitted		
	Pre-qualification bid	**Technical Bid**	**Financial Bid**
1	Bidder's Authorization Certificate**(Annexure-2)**	Technical Bid Covering Letter **(Annexure-5)**	Financial Bid Cover letter and Format **(Annexure-8)**
2	Particulars of the Bidder(**Annexure-1**)	Detailed Bill of material as per components indicated in Bill of Quantity. **(Annexure-11)**	Financial Bid **(Annexure-12)**
3	a. Valid copy of Certificate of incorporation and Registration Certificates b. Copy of GST registration. c. Copies of relevant Certificates of Registration, Income Tax/ PAN Number from the respective Government Department.	Technical Compliance with Relevant Supporting Documents	
4	Audited Balance Sheets		
5	CA Certificate with CA's Registration Number & Seal**(Annexure-8)**		
6	Valid ISO certificate		
7	Relevant Documents supporting Office addresses/Undertaking. (Local presence)		
8	RFP Form **(Annexure- 4)**		
9	MAF **(Annexure- 6)**		
10	Self-Declaration **(Annexure- 9)**		
11	Acceptance of Terms & Conditions of RFP **(Annexure- 15)**		
12	Project Citation Format**(Annexure- 10)**		
13	Project References (**Technical Capability)**		
14	**RFP document fee** as mentioned in the Eligibility/Pre-qualification Criteria of the RFP		
15	**EMD** as mentioned in the Eligibility/Pre-qualification Criteria of the RFP		

26. Annexure-15: Acceptance of Terms & Conditions

To,

The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of I.T. Dep't, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL,
Bhubaneswar - 751013
Sir,

I have carefully gone/examined through the Terms & Conditions mentioned in "Request for Proposal-for Implementation, Operations and Maintenance of OSWAN NOC" RFP Ref. No: OCAC-NEGP-INFRA-0007-2021-22061 Dated 23.08.2022 and I declare that all the previous/clause mentioned in this RFP Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Authorised Signatory
Name:
Designation:

Seal of The Company