

Request for Proposal



RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha

RFP Ref. No.: -OCAC-SEGP-INFRA-0002-2019-ENQ-23013



ODISHA COMPUTER APPLICATION CENTRE

[TECHNICAL DIRECTORATE OF E&IT DEPARTMENT, GOVERNMENT OF ODISHA]

OCAC Building, Acharya Vihar Square, Bhubaneswar-751013, Odisha, India

W: www.ocac.in | T: 0674-2567295/2567283 | F: 0674-2567842

Table of Contents

1	Glossary of Terms	5
2	Fact Sheet	6
3	Request for proposal	7
4	Structure of the RFP	7
5	Background Information.....	8
5.1	Basic Information	8
5.2	Project Background.....	8
5.2.1	About OCAC.....	8
5.2.2	Project Profile.....	8
6	Instruction to the Bidders.....	9
6.1	General.....	9
6.2	Compliant Proposals / Completeness of Response	9
6.3	Code of integrity	10
6.4	Pre-Bid Meeting and Clarifications	11
6.4.1	Pre-Bid conference.....	11
6.4.2	Responses to Pre-Bid Queries and Issue of Corrigendum	11
6.5	Key Requirements of the Bid	12
6.5.1	Right to Terminate the Process.....	12
6.5.2	RFP Document Fees.....	12
6.5.3	Earnest Money Deposit.....	12
6.6	Submission of proposal.....	13
6.6.1	Instruction to Bidders for Online Bid Submission	13
6.6.2	Guidelines for Registration	13
6.6.3	Searching for Tender Documents	14
6.6.4	Preparation of Bids.....	14
6.6.5	Submission of Bids.....	15
6.6.6	Clarifications on using e-Nivida Portal	16
6.6.7	Tender Validity	16
6.6.8	Submission and Opening of Proposals (electronic mode only)	16
6.6.9	Bids in other form	17
6.6.10	Proposal Preparation Costs	17
6.6.11	Language	17

6.6.12	Acceptance and Rejection of Bids	17
6.7	Evaluation Process	17
7	Criteria for Evaluation.....	18
7.1	Pre-Qualification Criteria	19
7.2	Technical Evaluation	22
7.3	Evaluation of Commercial Bids	23
8	Appointment of system integrator or Service provider.....	24
8.1	Award Criteria	24
8.2	Right to Accept Any Proposal and To Reject Any or All Proposal(s).....	24
8.3	Purchaser’s Procurement Rights.....	24
8.4	Notification of Award.....	25
8.5	Contract Finalization and Award.....	25
8.6	Performance Guarantee	25
8.7	Signing of Contract.....	26
8.8	Failure to Agree with the Terms and Conditions of the RFP	26
8.9	Contract Term	26
9	Terms of Reference (Scope of work)	27
9.1	Overview	27
9.2	Background	27
9.3	Present Design Architecture	30
9.4	Rationale	30
9.5	Proposed Solution.....	32
9.6	Project Kick–Off.....	32
9.7	Deliverables.....	32
9.8	Project Planning & Management.....	34
9.9	Functional requirements.....	36
9.9.1	Implementation Plan.....	36
9.9.2	Required features.....	36
9.9.2.1	General Requirement	36
9.9.2.2	External DNS Server.....	37
9.9.2.3	Internal DNS.....	38
9.9.2.4	DHCP	40
9.9.2.5	IPAM	41

9.10	Technical Support	42
9.11	Specification and features	43
9.12	Bill of Materials.....	49
9.13	Contract Period.....	50
9.14	Timeline and Penalty	50
9.14.1	Delivery, Installation and Commissioning	50
9.14.2	Penalty for Non-Availability/Downtime of Service	50
9.14.3	Other Penalty terms.....	50
9.15	Payment term	51
9.15.1	Appliance Cost	51
9.15.2	License Cost	51
9.15.3	Installation and Commissioning.....	51
9.15.4	Warranty support and subscription cost.....	51
9.15.5	Support Resource cost.....	51
10	Formats for Response.....	52
10.1	Pre-Qualification Bid Formats	52
10.1.1	FORM PQ-1: Cover Letter	52
10.1.2	FORM PQ-2: Bidder’s Organization (General Details)	53
10.1.3	FORM PQ-3 [Acceptance of Terms and Conditions].....	54
10.1.4	FORM PQ-4 [Self-Declaration against Not-Blacklisted]	55
10.1.5	FORM PQ-5: Project Citation Format	56
10.1.6	FORM PQ-6: Bidder’s Authorization Certificate	57
10.1.7	Format for Bank Guarantee for Earnest Money Deposit	58
10.2	Technical Bid Formats.....	60
10.2.1	FORM TECH-1:.....	60
10.2.2	FORM TECH-3:.....	61
10.2.3	FORM TECH-4: Support Structure.....	62
10.3	Financial Bid.....	63
10.3.1	FORM FIN-1: Financial Bid Covering Letter	63
10.3.2	Commercial bid	65
10.3.3	Performance Security	67
11	Proposed Master Service Agreement	69

1 Glossary of Terms

BG	Bank Guarantee
BCP	Business Continuity Plan
BHQ	Block Headquarters
DDI	DNS-DHCP-IPAM Solutions
DHCP	Dynamic Host Configuration Protocol
DHQ	District Headquarters
DNS	Domain Name System
E&IT	Electronics and Information Technology
EMD	Earnest Money Deposit
e-Nivida	e-Procurement Platform Solution
ICT	Information and Communication Technology
IMAP	Internet Message Access Protocol
IPAM	IP Address Management
ITES	Information Technology Enabled Services
L1 Bidder	Bidder with L1(Lowest) Quote
L1 quote	Lowest price discovered through Commercial Bid
LCBS	Least Cost Based Selection
OCAC	Odisha Computer Application Centre
OSWAN	Odisha State Wide Area Network
PBG	Performance Bank Guarantee
RFP	Request For Proposal
SDC	State Data Centre
SHQ	State Headquarters
SI	System Integrator
SP	Service Provider/Solution Provider
TOR	Terms of Reference
VC	Video Conferencing

2 Fact Sheet

Sl#	Item	Description
a)	Project Title	RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha
b)	Name of Purchaser	Odisha Computer Application Centre
c)	Contact Person, Address and Email	General Manager (Admin) Plot No. N-1/7-D, Acharya Vihar RRL Post Office, Bhubaneswar Odisha - 751013 gm_ocac@ocac.in
d)	RFP Document Fees	₹11,200/- inclusive of GST @ 12% (Rupees Eleven Thousand and Two Hundred only)
e)	Earnest Money Deposit	₹15,00,000/- in shape of DD/RTGS or BG
f)	Selection Method	Least Cost Based Selection (LCBS)
g)	Last date for submission of queries by Bidders	By 4 PM of 23.03.2023
h)	Pre-bid Meeting	24.03.2023 at 12 Noon (in VC mode)
i)	Last date and time for receipt of proposals from Bidders	11.04.2023 by 12 Noon through e-Nivide Portal (www.enivida.odisha.gov.in)
j)	Date and time for opening of Technical Proposals	11.04.2023 by 12:30
k)	Date and time for Technical Presentation	To be notified later
l)	Date and time for opening of Commercial Bids	To be notified later
m)	Bid Validity Period	180 Days
n)	Project Term	Contract duration would be 64 months from the date of work order

3 Request for proposal

Sealed proposals are invited from eligible, reputed, qualified System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha for a period of 6 years from the date of commissioning of service. The details of scope of work is mentioned in the Terms of Reference section of this Request for Proposal (RFP) Document. This invitation to bid is open to all bidders meeting the minimum eligibility criteria as mentioned in this RFP Document.

4 Structure of the RFP

This RFP document for “RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha)” comprises of the following.

- a) Instructions on the Bid process for the purpose of responding to this RFP. This broadly covers:
 - i) General instructions for bidding process
 - ii) Bid evaluation process including the parameters for Pre-qualification, Technical Evaluation and Commercial Evaluation for determining bidder’s suitability as the system integrator
 - iii) Commercial bid and other formats
- b) Functional and Technical Requirements of the project. The contents of the document broadly cover the following areas:
 - i) About the project and its objectives
 - ii) Scope of work
 - iii) Timeline
 - iv) Service levels

The bidder is expected to respond to the requirements as completely and in as much relevant detail as possible and focus on demonstrating bidder’s suitability to become the System Integrator of OCAC for this assignment.

The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP documents. Failure to furnish all information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the bidder's risk and may result in rejection of the proposal.

5 Background Information

5.1 Basic Information

OCAC, the technical directorate of E & IT Department, Government of Odisha invites responses (“Tenders”) to this Request for Proposals (“RFP”) from System Integrators (“Bidders”) for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha as described in this RFP, “Terms of Reference”.

Proposals must be received not later than time, date and venue mentioned in the Fact Sheet.

Proposals that are received late will not be considered in this procurement process.

OCAC will award the Contract to the successful bidder whose proposal has been determined as the best value proposal based on Technical and Financial evaluation criteria and accepted by the Tender Accepting Authority.

5.2 Project Background

5.2.1 About OCAC

The Department of Electronics & Information Technology is the nodal department for Government of Odisha in the matters of IT, ITES and Communication. The department plays a vital role in formulating and implementing policy matters in Information Technology, ITES, Electronics and Telecom; promotion of Odisha as an ultimate ICT destination for investment and facilitating ICT industries; assisting other department for effective e-Governance and capacity building; Promotion of ICT based education in the State.

Odisha Computer Application Centre (OCAC), the Technical Directorate of Electronics & Information Technology Department, Government of Odisha, has evolved through years as a centre of excellence in IT solutions and e-Governance. It has contributed significantly to the steady growth of IT in the state. It helps IT to reach the common citizen so as to narrow down the Digital Divide and widespread applications of IT in establishing a system where the citizens are receiving good governance in addition to ensuring speed of decisions from a transparent Government through an effective e-Governance System.

5.2.2 Project Profile

Odisha Computer Application Centre (OCAC) is trying its best efforts to protect against the compromise of organizations’ perimeter defenses. Looking at today’s malware is more sophisticated than earlier. Evolving quickly, it can evade discovery after it has

compromised a system while providing a launching pad for a persistent attacker to move throughout an organization.

The proposed solution should offer deep visibility, context, and control to rapidly detect, contain, and remediate advanced threats if they evade front-line defenses. It should extend beyond prevention capabilities and addresses the full lifecycle of the advanced malware problem, i.e. Prevention, Detection and Response.

The Bidder is required to do provisioning of setup DNS server with security. Under this solution, the bidder is expected to provide the software and/or appliances separately and include the pricing under the same line item. Detailed technical specification is available for functional requirements. The bidder is required to provide all the software/appliance based on the technical specification. Both the software/appliances should be installed and configured as per the requirement of OCAC. Bidder and OEM are responsible for the same. OEM is required to certify the solution installed configure as per best industry practice and that there is no gap in the configuration part.

6 Instruction to the Bidders

6.1 General

- a) While efforts have been made to provide comprehensive and accurate background information, requirements and specifications, Bidders must form their own conclusions about the solution needed to meet requirements. Also, bidders may wish to consult their own legal advisers in relation 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 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 OCAC.
- d) This RFP supersedes and replaces any previous public documentation and communications, and Bidders should place no reliance and dependence on such communications.

6.2 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 of this paragraph may render the Proposal non-compliant and the Proposal may be rejected. Bidders must:
- Include all documentation specified in this RFP.
 - Follow the format of this RFP and respond to each element in the order as set out in this RFP.
 - Comply with all requirements as set out within this RFP.

6.3 Code of integrity

No official of a procuring entity or a bidder shall act in contravention of the codes which includes

- a. prohibition of
 - i. Making offer, solicitation or acceptance of bribe, reward or gift or any material benefit, either directly or indirectly, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process.
 - ii. Any omission, or misrepresentation that may mislead or attempt to mislead so that financial or other benefit may be obtained or an obligation avoided.
 - iii. Any collusion, bid rigging or anticompetitive behavior that may impair the transparency, fairness and the progress of the procurement process.
 - iv. Improper use of information provided by the procuring entity to the bidder with an intent to gain unfair advantage in the procurement process or for personal gain.
 - v. Any financial or business transactions between the bidder and any official of the procuring entity related to tender or execution process of contract; which can affect the decision of the procuring entity directly or indirectly.
 - vi. Any coercion or any threat to impair or harm, directly or indirectly, any party or its property to influence the procurement process.
 - vii. Obstruction of any investigation or auditing of a procurement process.
 - viii. Making false declaration or providing false information for participation in a tender process or to secure a contract;
- b. Disclosure of conflict of interest.
- c. Disclosure by the bidder of any previous transgressions made in respect of the provisions of sub-clause (a) with any entity in any country during the last three years or of being debarred by any other procuring entity.

In case of any reported violations, the procuring entity, after giving a reasonable opportunity of being heard, comes to the conclusion that a bidder or prospective bidder, as the case may be, has contravened the code of integrity, may take appropriate measures.

6.4 Pre-Bid Meeting and Clarifications

6.4.1 Pre-Bid conference

- a) OCAC shall hold a pre-bid meeting with the prospective bidders on **24.03.2023 at 12 Noon in VC Mode** (through Microsoft Teams).
- b) Link will be provided to the interested bidders on request through email to gm_ocac@ocac.in (with a copy to subrat.mohanty@ocac.in and debaraj.behera@ocac.in) by **4 PM of 24.03.2023**.
- c) The representatives of Bidders (restricted to three persons) may attend the Pre-bid meeting.
- d) The Bidders should submit their queries in writing in below specified format (in MS-Excel only) by the schedule as mentioned in this RFP, prior to attending the pre-bid meeting.

Sl#	RFP Document Reference(s) (Section & Page Number(s))	Content of RFP requiring Clarification(s)	Points of Clarification

- e) OCAC shall not be responsible for any Bidders' queries received by it in any other format. Any requests for clarifications post the indicated date and time mentioned will not be entertained by OCAC.

6.4.2 Responses to Pre-Bid Queries and Issue of Corrigendum

- a) The Nodal officer notified by OCAC will endeavor to provide timely response to all queries. However, OCAC neither makes 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 Bidders.
- b) At any time prior to the last date for receipt of bids, OCAC may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP document by corrigenda and/or addenda.
- c) The Corrigendum (if any) and clarifications to the queries from all Bidders will be posted on www.enivida.odisha.gov.in, www.ocac.in or www.odisha.gov.in
- d) Any such corrigenda and/or addenda shall be deemed to be incorporated into this RFP.
- e) In order to provide prospective Bidders reasonable time for taking the corrigenda

and/or addenda into account, OCAC may, at its discretion, extend the last date for the receipt of Proposals

6.5 Key Requirements of the Bid

6.5.1 Right to Terminate the Process

- a) OCAC may terminate the RFP process at any time and without assigning any reason. OCAC makes no commitments, express or implied, that this process will result in a business transaction with anyone.
- b) This RFP does not constitute an offer by OCAC. The Bidder's participation in this process may result in OCAC selecting the Bidder to engage towards execution of the contract.

6.5.2 RFP Document Fees

The bidder must furnish along with its bid required bid document fee amounting to ₹11,200/- inclusive of GST @ 12% online through e-Nivida portal/or in shape of DD in favor of “Odisha Computer Application Centre” payable at Bhubaneswar.

The fee can also be paid through electronic mode to the following:

Bank A/c No: 149311100000195
Payee Name: Odisha Computer Application Centre
Bank Name & Branch: Union Bank of India, Acharya Vihar, Bhubaneswar
Account Type: Savings
IFSC: UBIN0814938

6.5.3 Earnest Money Deposit

- a) Bidders shall submit, along with their Bids, EMD of **₹15,00,000/-** (Fifteen Lakhs) in the shape of Bank Draft **OR** Bank Guarantee (in the format specified in this RFP at Clause no. 10.1.7) issued by any scheduled bank in favour of Odisha Computer Application Centre, payable at Bhubaneswar, and should be valid for 180 days from the due date of the tender / RFP. The EMD should be submitted in the General Bid.
- b) The EMD may also paid through electronic mode to the following financial

Bank A/c No. : 149311100000195
Payee Name : Odisha Computer Application Center
Bank Name & Branch : Union Bank of India, Acharya Vihar, Bhubaneswar
Account Type : Savings
IFSC : UBIN08 <u>14938</u>

- c) EMD of all unsuccessful bidders would be refunded by OCAC within 60 days of the bidder being notified as being unsuccessful. The EMD, for the amount mentioned above, of successful bidder would be returned upon submission of Performance Bank Guarantee.
- d) The EMD amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.
- e) The bid / proposal submitted without EMD, mentioned above, will be summarily rejected.
- f) The EMD may be forfeited:
 - i) If a bidder withdraws its bid during the period of bid validity.
 - ii) In case of a successful bidder, if the bidder fails to sign the contract in accordance with this RFP.
 - iii) If found to have a record of poor performance such as having abandoned work, having been black-listed, having inordinately delayed completion and having faced Commercial failures etc.
 - iv) The Bidder being found to have indulged in any suppression of facts, furnishing of fraudulent statement, misconduct, or other dishonest or other ethically improper activity, in relation to this RFP
 - v) A Proposal contains deviations (except when provided in conformity with the RFP) conditional offers and partial offers.

6.6 Submission of proposal

6.6.1 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>

6.6.2 Guidelines for Registration

- a) Bidders are required to enroll 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.2,800/- + 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.

6.6.3 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.

6.6.4 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.

6.6.5 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 BOQ 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 BOQ 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 BOQ 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.

6.6.6 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

Email id: odishaenivida@gmail.com

www.enivida.odisha.gov.in

6.6.7 Tender Validity

Proposals shall remain valid for a period of 120 Days from the date of opening of the pre-qualification and technical proposals. OCAC reserves the rights to reject a proposal valid for a shorter period as non-responsive and will make the best efforts to finalize the selection process and award of the contract within the bid validity period. The bid validity period may be extended on mutual consent.

6.6.8 Submission and Opening of Proposals (electronic mode only)

- a) The bidders should submit their responses as per format given in this RFP in the following manner:
 - Response to Pre-Qualification Criterion
 - Technical Proposal
 - Commercial Proposal
- b) Please Note that Prices should not be indicated in the Pre-Qualification Response or Technical Proposal but should only be indicated in the Commercial Proposal.
- c) The Response to Pre-Qualification criterion, Technical Proposal and Commercial Proposal (as mentioned in previous paragraph) should be submitted through online mode in e-Nivida Portal.

The Proposals submitted up to 11.04.2023 by 12 noon will be opened on 11.04.2023 at 12:30 PM by Proposal Evaluation Committee .

6.6.9 Bids in other form

- a) The bids submitted in hard copy or by post/e-mail etc. shall not be considered and no correspondence will be entertained on this matter.
- b) OCAC reserves the right to modify and amend any of the above-stipulated condition/criterion depending upon project priorities vis-à-vis urgent commitments.

6.6.10 Proposal Preparation Costs

The bidder shall be responsible for all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings or discussions or presentations, preparation of Proposal, 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.

6.6.11 Language

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 Bidders. For purposes of interpretation of the Proposal, English translation shall govern.

6.6.12 Acceptance and Rejection of Bids

OCAC reserves the right to reject in full or part, any or all bids without assigning any reason thereof. OCAC reserves the right to assess the Bidder's capability and capacity. The decision of OCAC shall be final and binding. Bid should be free of overwriting. All measures, correction or addition must be clearly written both in words and figures and attested. Offers not submitted in prescribed manner or submitted after due date and time are liable to rejection.

6.7 Evaluation Process

- a) OCAC will constitute a Proposal Evaluation Committee to evaluate the responses of the bidders.
- b) The Proposal Evaluation Committee constituted by OCAC shall evaluate the

responses to RFP and all supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence, may lead to rejection of the bid.

- c) The decision of Proposal Evaluation Committee in evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of negotiation/ discussion with the Committee.
- d) The Proposal Evaluation Committee may ask for meetings with the Bidders to seek clarifications on their proposals, if required.
- e) The Proposal Evaluation Committee reserves the right to reject any or all proposals on the basis of any deviations.
- f) Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.
- g) Initial bid scrutiny will be held, and incomplete details as given below will be treated as nonresponsive if proposals are:
 - Not submitted as specified in the RFP document
 - Received without the Letter of Authorization (Power of Attorney)
 - Found with suppression of details
 - Found with incomplete information, subjective, conditional offers and partial offers submitted
 - Submitted without the documents requested in checklist
 - Submitted with lesser validity period
- h) All responsive Bids will be considered for further processing as below:

OCAC will prepare a list of responsive bidders, who comply with all the Terms and Conditions of RFP. All eligible bids will be considered for further evaluation by a Committee according to the evaluation process defined in this RFP document. The decision of the Committee will be final in this regard.

7 Criteria for Evaluation

The overall objective of this evaluation process is to select the capable and qualified firm and providing associated capacity building, training and operations & maintenance support.

The Pre-Qualification proposal will be evaluated as per criteria mentioned below and only those bidders who qualify the requirements will be eligible for next set of evaluations. Technical Proposal and Commercial Proposal of Bidders who do not meet the Pre-Qualification criteria will not be opened in the portal.

The technical score of all the bidders would be calculated as per the criteria mentioned below. All the bidders who achieve more than 70 marks in the technical evaluation would be eligible for the next stage, i.e. Commercial Bid opening.

Bidders should submit supporting documentary evidence with respect to the above, in absence of which their proposals will be summarily rejected.

7.1 Pre-Qualification Criteria

Sl#	Basic Requirement	Specific Requirement	Documents required
1.	Legal Entity	The bidder must be a company registered in India under Indian Companies Act 1956/2013 OR A Partnership firm registered under Indian Partnership Act, 1932, The bidder must be in operation in India since last 5 years as on 31st December 2022. The bidder must have GST registration & up-to-date Income Tax Return, Valid PAN Number as on 31st March 2022.	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
2.	Turnover	The average annual turnover of the bidder during the last three financial year ending with 2021-22 should not be less than ₹ 40 Crore from IT/ITeS (as per the last published audited balance sheets / CA certified provisional balance sheet).	- Audited Balance Sheets along with CA Certificate showing average turnover.
3.	Net Worth	The net worth of the bidder in the last three financial year ending on 31st March 2022, (as per the last published audited balance sheet/ CA certified provisional balance sheet) should be Positive.	- CA Certificate
4.	OEM Experiences	OEM should have implemented at least 5 heterogeneous setups (means BFSI, Government /PSU/Autonomous body, Telecom companies).	Customer PO copies, completion certificate and any feedback from the client.

5.	Bidder Technical Capability	<p>The bidder/OEM must have successfully undertaken at least 5 heterogeneous setup (means BFSI, Government/ PSU/ Autonomous body, Telecom companies) the following numbers of similar assignments of value specified herein:</p> <ul style="list-style-type: none"> - Minimum one project of similar nature, not less than the amount of ₹8,00,00,000/- (Eight Crore Only) <p>or</p> <ul style="list-style-type: none"> - Minimum two projects of similar nature, not less than the amount of ₹6,00,00,000/- (Six Crore Only) <p>or</p> <ul style="list-style-type: none"> - Minimum three projects of similar nature, not less than the amount of ₹4,00,00,000/- (Four Crore Only) 	<p>Copy of Work Order/PO + Self Certificate of satisfactory work completion certificate/ work in progress.</p> <p>Also, along with the above document, share the Customer Name, designation and Phone number for cross reference.</p>
6.	Quality Certification	The bidder must possess a valid ISO 9001, ISO20001 & ISO27001 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	<p>The bidder must attach Manufactures Authorization certificate specific to this tender & Back-to-back support letters from OEMs for providing Comprehensive support and services of the OEM's product covered under the RFP.</p> <p>MAF should contain the details of authorised signatory which includes Full name, designation, mobile no., email id) and should be digitally signed.</p>	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 the establishment of an office, within one month of the award of the contract.	Relevant Documents supporting office addresses/ Undertaking.
10.	Document Fee	The bidder must have made a payment of ₹11,200.00 (Rupees Eleven Thousand Two Hundred Only) (Inclusive of GST) towards tender document fee.	Online at e-Nivida Portal
11.	EMD	₹20,00,000/- in shape of DD or BG	

7.2 Technical Evaluation

- 7.2.1 Bidder must quote all the products/equipment mentioned in the Bill of Materials. Otherwise, the bid will not be considered.
- 7.2.2 Bidder must furnish tender-specific Manufacture Authorisation Form against the entire item mentioned in the Bill of Material.
- 7.2.3 Bidder must furnish the unpriced bill of materials of the items quoted in the technical bid.
- 7.2.4 Bidder should accept the entire scope of work (including services) as mentioned in the Scope of work.
- 7.2.5 The Bidder/OEM must have experience with the Proposed DDI solution (DNS, DHCP& IPAM) and should be implemented and running in Public/Government entity in India. (The bidder my Copy of original PO / Contract Completion Certificate or Installation Report or Credential letter from client working specifying project completion).
- 7.2.6 The Product offered should meet all the technical and functional specifications given in the “Specification Section”
- 7.2.7 All the compliances should be submitted on OEM Letterhead.
- 7.2.8 Response except “Yes” or “No” is not acceptable. If any bidder provides response other than “Yes” or “No” the same will be treated as Not Available i.e. NA.
- 7.2.9 The bidder should furnish documentation in technical bid and make demonstration/presentation on the proposed solution as per following parameters before bid evaluation committee. Based on the documentation and presentation/demonstration mark shall be awarded.

Sl#	Evaluation Criterion	Max Score	Documents Required
i)	<p>Technical evaluation will be evaluated on the following parameters (apart from compliance of the product quoted) :</p> <ul style="list-style-type: none"> a. Design Architecture of Proposed Solution b. Resilience of proposed architecture, approach and methodology c. Future scalability d. Security Aspects 	50	<ul style="list-style-type: none"> – Technical document – Presentation and Demonstration

Sl#	Evaluation Criterion	Max Score	Documents Required
	<p>Presentation and product demonstration on in-depth understanding of the proposed project's technical and functional requirements. Major Criteria for demonstration (but not limited to) are given as under:</p> <ul style="list-style-type: none"> • Bidder's understanding on project scope. • Bidder's knowledge and experience to deliver vis-à-vis scope of the assignment. • Project timeline, implementation framework on the proposed solution • Bidder's ability to provide crisp and clear answers with strong content 		

7.2.10 Bidders, whose bids are responsive to all the items in the Compliance Sheet for Technical Proposal and meet all the technical and functional specifications, and secured more than 70% mark in the technical documentation and presentation would be considered technically qualified.

7.2.11 The commercial bids of only the technically qualified bidders will be opened for further processing.

7.3 Evaluation of Commercial Bids

- a) Bidders will be selected through Least Cost Based Selection Process (L1).
- b) The Commercial Bids of technically qualified bidders (i.e. Bidders with more than 70 marks in Technical Evaluation) will be opened on the prescribed date in the presence of bidder representatives.
- c) Only fixed price financial bids indicating total price for all the deliverables and services specified in this bid document will be considered.
- d) The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately.
- e) The Bidder, who has submitted the lowest Commercial bid (i.e. lowest in grand total), shall be selected as the L1 and shall be called for further process leading to the award of the assignment.

- f) Any conditional bid would be rejected.
- g) Errors & Rectification: Arithmetical errors will be rectified on the following basis: “If there is a discrepancy between the unit price and total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail. If the bidder does not accept the correction of error, its bid will be rejected”.
- h) If there is no price quoted for certain material or service, the bid shall be declared as disqualified.
- i) In the event that there are 2 or more bidders having the same value in commercial bid, the bidder securing highest technical score will be adjudicated as “Best responsive bid” for award of the Project.

8 Appointment of system integrator or Service provider

8.1 Award Criteria

Purchaser will award the Contract 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.

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

OCAC reserves the right to accept or reject any proposal, and to annul the tendering process/ public procurement process and reject all proposals 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 OCAC action.

8.3 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) Exclude any of the module(s)
- e) Remove any of the items at the time of placement of order.
- f) Increase or decrease no. of resources supplied under this project.
- g) Should the Purchaser be unsuccessful in negotiating a contract with the selected

bidder, the Purchaser will begin contract negotiations with the next best value bidder in order to serve the best interest.

- h) Make typographical correction or correct computational errors to proposals
- i) Request bidders to clarify their proposal

8.4 Notification of Award

Prior to the expiration of the proposal 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 formation of the Contract. Upon the successful bidder's furnishing of Performance Bank Guarantee (PBG), OCAC will notify each unsuccessful bidder and return their EMD.

8.5 Contract Finalization and Award

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 contract agreement would be finalized for award & signing.

8.6 Performance Guarantee

- a) OCAC will require the selected bidder to provide a Performance Bank Guarantee (PBG), within 15 days from the date of notification of award.
- b) The bidder should furnish PBG amounting to 10% of work order value excluding tax in favour of OCAC valid for 68 months as per format attached at clause 10.3.4
- c) The selected bidder 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 service during the work order period.
- d) In case the selected bidder fails to submit performance guarantee within the time stipulated, OCAC at its discretion may cancel the order placed on the selected bidder after giving prior written notice to rectify the same.
- e) 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.

8.7 Signing of Contract

After OCAC notifies the successful bidder that its proposal has been accepted, OCAC shall enter into a contract with the successful bidder (prime bidder in case of consortium), incorporating all clauses, pre-bid clarifications and proposal of the bidder.

A draft MSA document has been provided as a separate document for the reference of bidders only. The agreement with the selected bidder will be signed after getting the same vetted from competent Legal Authority.

8.8 Failure to Agree with the Terms and Conditions of the RFP

Failure of the successful bidder to agree with the draft legal agreement and Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of award, in which event OCAC may call for new proposals from the interested bidders. In such a case, OCAC shall invoke the PBG of successful bidder.

8.9 Contract Term

Contract duration would be 64 months from the date of issuance of work order i.e. 4 months of supply, configuration, installation and commissioning and 60 months of operation and maintenance support from the date of commissioning.

9 Terms of Reference (Scope of work)

9.1 Overview

Odisha Computer Application Centre (OCAC) is trying its best efforts to protect against the compromise of organizations' perimeter defenses. Looking at today's malware is more sophisticated than earlier. Evolving quickly, it can evade discovery after it has compromised a system while providing a launching pad for a persistent attacker to move throughout an organization.

The proposed solution should offer deep visibility, context, and control to rapidly detect, contain, and remediate advanced threats if they evade front-line defenses. It should extend beyond prevention capabilities and addresses the full lifecycle of the advanced malware problem, i.e. Prevention, Detection and Response.

The Bidder is required to do provisioning of setup DNS server with security. Under this solution, the bidder is expected to provide the software and/or appliances separately and include the pricing under the same line item. Detailed technical specification is available for functional requirements. The bidder is required to provide all the software/appliance based on the technical specification. Both the software/appliances should be installed and configured as per the requirement of OCAC. Bidder and OEM are responsible for the same. OEM is required to certify the solution installed configure as per best industry practice and that there is no gap in the configuration part.

9.2 Background

Odisha Computer Application Centre is the nodal agency of Odisha State working towards the promotion & implementation of IT and e-Governance. It is the single point of access to any IT business opportunity in Odisha and encourages various players in the field of IT to come forward and invest in the State of Odisha. OCAC is committed to generating IT business for the public/private sector with a mandate from the Government to develop IT in the state. This includes opportunities for software development, supply of hardware & peripherals, networking and connectivity, web applications, e-commerce, IT training and an entire gamut of direct and indirect IT businesses.

As part of the overall initiatives of e-Governance, the Government of Odisha through OCAC has created the network infrastructure at Secretariat Campus and associated Government Offices for data, Voice, Video communication and Internet access.

Besides, there is a Portal Data Centre that houses various e-Governance applications and provides hosting services to various Government Departments/ Offices.

OCAC has also established a Portal Data Centre consisting of web servers, application servers, data servers on cluster mode, firewall, storage, DNS Server, proxy servers, Routers, Modems etc. to provide hosting facilities to Government Departments/ Offices. The list of services under SecLAN is listed here:

- a. Managed hosting services for websites/ web applications.
- b. E-mail services
- c. Internet gateway
- d. DNS services
- e. SAN Storage Services
- f. Backup and restore services

OSWAN

A wide area network deployed in the State has two components viz.

- Vertical Component
- Horizontal Component

The vertical component of SWAN is implemented using multi-tier architecture (typically, three-tier) with the State/UT Headquarter (SHQ) connected to the each District Head Quarter (DHQ) which in turn gets connected to each Block Head Quarter (BHQ). Each SHQ, DHQ and BHQ point of connection is called a Point of Presence (PoP), which is a point of bandwidth aggregation for several network links getting connected at this point. The bandwidth provisioning for network connectivity between all the above PoPs is a minimum of 2 Mbps. Presently, the connectivity provisioning between every SHQ and DHQ is for 4 Mbps and DHQ to every BHQ is 2 Mbps. For the horizontal component, the government departments at each tier are connected to the respective PoPs

The SWAN aims to create a dedicated Closed User Group (CUG) network of minimum speed of 2 Mbps by connecting around 7500 pops, providing Data, Voice & Video connectivity to more than 50,000 govt. offices. The networks aim at increasing the efficiency of the government delivery mechanism and optimizes the performance. The backbone thus created would provide reliable, vertical and horizontal connectivity within the State / UT administration and would facilitate electronic transactions between all the government departments.

OSWAN's 315 Vertical PoP

SHQ	01
DHQ	30
Block HQ	284
Total	315

OSWAN's 61 Horizontal PoP

SHQ Bhubaneswar	20
DHQ Cuttack	15
DHQ Berhampur	12
DHQ Sambalpur	14
Total	61

SDC

The State Data Centre (SDC) is a key-supporting pillar of e-Government initiatives for delivering services to the citizens with greater reliability, availability and serviceability. SDC provides better operations & management control and minimizes overall cost of Data Management, IT Management, Deployment and other costs.

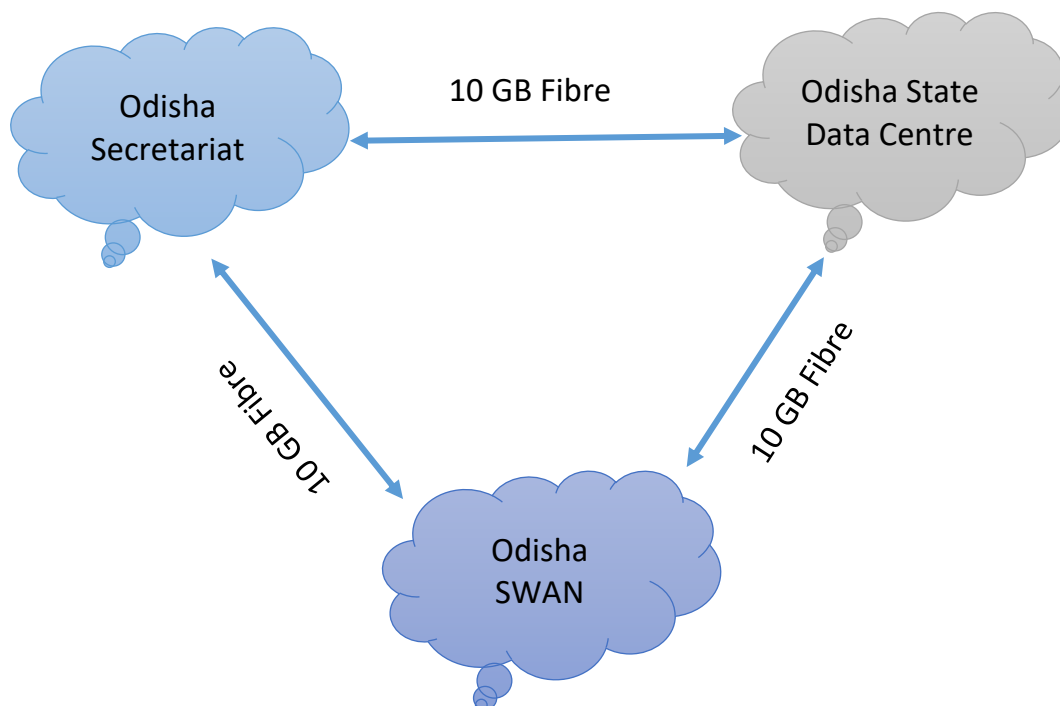
Ministry of Information Technology and Electronics (MeitY), Government of Odisha (GoO) were the key and core stakeholder of the implementation of various Mission Mode Projects under NeGP. A Composite Team has been formed with the officers from OCAC and the National Informatics Centre (NIC) for shouldering the responsibility of techno-administrative support of overall SDC operations, management and hosting various departmental applications at SDC.

To extend the success of computerization, the Government of Odisha (GoO) in support with its nodal agency set up SDC for hosting the departmental applications. Presently, the Data Centre is catering to the IT infrastructural needs of all departmental-owned applications and e-Governance applications envisaged to provide a wider range of services to the Citizens of Odisha by computerizing the operations of various departments of GoO.

9.3 Present Design Architecture

There are basically three different sites i.e. Odisha Secretariat, Odisha SWAN and Odisha State Data Centre interconnected with 10G fibre link. Presently all three different verticals have their own operational boundary. All three sites are accessing most of the common applications are hosted in SDC and Secretariat. All three sites having their own silo DNS Server. However, accessing to the internet is independent.

Present connectivity is like below



9.4 Rationale

Apart from the various activities like domain (Parent/Child) registration, network allocation, e_despatch and OSWAS depend upon DNS, Monitoring and Evaluation is an important component that needs to be undertaken through the implementation of DHCP, DNS and IPAM (DDI). Since all the above three sites are running with their silo DNS, sometimes managing such distributed DNS could not be easy to manage from a single dashboard. The Domain Name System (DNS) is a centralized system used by various organizations to translate domain names into IP addresses. It is an important service as it takes too much time to remember IP addresses instead of URLs or to manually configure all devices in a larger network. DNS security threats are among the most common types of cyber threats that occur today. DNS security should be an integral part of a state's security plan. Based on the above scenario Odisha Computer

Application Centre desires to implement a Global standard DDI platform which is imperative for the below-mentioned considerations:

1. The DNS log is a common infrastructure service used by all protocols. The DNS log contains the credentials for all services used in the corporate network. For example, you can get information about the protocol of web traffic only on the proxy server and about the log of e-mail traffic only on the e-mail server. The DNS log contains data about both types of traffic. Therefore, processing the DNS log means processing the entire corporate network.
2. Malicious traffic without IP address can be detected only through the DNS log. Examples of domain types without IP addresses include:
 - a. According to Cyber X-Ray data, it was found that about 85% of malware domains do not have a direct IP address. Since there is no IP address, there is no HTTP request and since there is no log, it is only necessary to analyze the DNS log.
 - b. DGA domain: these are domains created with a special algorithm depending on the system clock. These domains are registered only when the zombie network is commanded and has the IP address. The owner of the zombie army has two goals: (i) Prevent command center connection domains from being discovered by security researchers, (ii) Unlock the zombie army on a timed basis
 - c. DNS tunneling: With DNS tunneling, data theft cannot be detected by DLP products. DNS tunneling data can only be detected by analyzing the DNS log.

Effectively monitoring DNS traffic on your network for suspicious anomalies is critical to early detection of a security breach. By implementing State Level DNS, can keep an eye on all the important metrics. With intelligent SIEM integration, you can set up alerts for a specific time period or as a result of a combination of abnormal actions. DNSSEC artificial intelligence algorithms ensure a classification rate of over 99.5%. Based on this database, it sends only the data to SIEM that needs to be investigated by Soc teams. Thus, intelligent SIEM integration can save more than 95% of DNS log processing costs.

The DDI platform is to be carried out to visualise and explore the impact and status of the utilisation and threat landscape of multiple sites. The implementation mechanism includes analysis of institutional arrangements, and bottlenecks if any in the process of implementation and recommends suitable measures for effective deployment on a

per-need-to-need basis. The said implementation would check the all-around achievement of the usage of resources and impact, future best practices to change the policy improvements. It is to be noted that all three sites have their own IP address allocation mechanism.

To address better IP address management and monitoring DDI will be helpful to manage centrally. This could help to avoid IP address conflict and swapping from a single dashboard. Following the best strategy interoperability of sites could be tested through central IP address management.

9.5 Proposed Solution

Modern infrastructures are the foundation of key IT transformation initiatives: hybrid cloud, multi-cloud, SD-WAN, Zero Trust, zero-touch networks, mobility, IoT, and more. These global trends are adding extreme pressure on network services, regardless of size, complexity, and business/service focus.

To simplify management, enhance the efficiency of operations, and accelerate time to provide service proactively, Odisha Computer Application Centre (OCAC) has decided to bring high-performance solutions for critical DNS-DHCP-IPAM services. Which provides vital benefits for, the reliability, resiliency, and security of network foundations from a single dashboard. The Minimum Technical Specification is described in the functional requirement.

9.6 Project Kick-Off

During Project Setup & Initiation stage, the vendor will designate a nodal person to serve as the single point of contact for the Project. The project managers will:

- i. Develop a Project Schedule
- ii. Conduct a Project Kick-Off meeting to introduce all stakeholders
- iii. Conduct risk assessment
- iv. Deliver Kick-off Presentation
- v. Document and Obtain Sign-off on Project Plan

9.7 Deliverables

- Project Inception Report/ Delivery report
- IT Infrastructure Requirements Definition

During this stage, the vendor will coordinate with all stakeholders to gather the requirements:

- i. Identify and define installation requirements
- ii. Identify and define inter-connection/integration requirements

- iii. Any other requirement to complete the scope of work

Schedule Deliverables

No	Items	Site/Location	Timeline in days
1	Supply / Delivery of Software of the solution	Individual Location	T+12 weeks after the issue of the PO
2	Installation and commissioning		T+16 weeks
3	Documentation and manuals	Individual location	Within 7 days of the operational acceptance

The Implementation Agency shall ensure that the solution is thoroughly tested as per the standard process defined hereunder or by OCAC should the process evolve over the contract period. OCAC requires a thorough and well-managed test methodology to be conducted. The Implementation Agency must build up an overall plan for testing and acceptance of the system, in which specific methods and steps should be clearly indicated and approved by OCAC. The Implementation Agency is required to incorporate all suggestions/feedback provided after the elaborate testing of the IT Infrastructure/Solutions supplied, within a pre-defined, mutually agreed timeline. Bidder is expected to provide the manpower for installation and commissioning and support for five years from the date of commissioning. OCAC will confirm to depute the manpower for doing this activity if required. There will not be any additional cost for this process.

The Implementation Agency shall undertake the following broad-level activities:

- i. Outline the methodology that will be used for testing and fine-tuning the system from time to time
- ii. Define the various levels or types of testing that will be performed for the system
- iii. Provide the necessary checklist/documentation that will be required for testing the system
- iv. Describe any techniques, test cases/scenarios/scripts that will be used for testing the system
- v. Describe how the testing methodology will conform to the requirements of each of the functionalities

- vi. Indicate/demonstrate to OCAC that all desired Software/Applications installed in the system have been tested
- vii. The vendor shall provide a workflow for sign-off on test deliverables that is mutually agreed by both parties
- viii. User acceptance certificate should be provided by the vendor.

Competent Authority from OCAC shall issue an appropriate acceptance certificate to the Implementation Agency for the successful roll-out of the application. The testing levels should include Unit Testing, Integration Testing, System Testing and Acceptance Testing (including performance testing and fine-tuning). These tests should be included such as security testing, performance testing, Usability testing, Concurrency testing, etc. The Implementation Agency must work with OCAC to provide a detailed deployment plan, including but not limited to, application version control, loading all application materials, assignment of user rights and security, and verification of correct functionality.

An Operational Acceptance shall commence on the system, once the system is commissioned for a period of maximum 15 days. Operational Acceptance will only be provided after UAT has been performed, and sign-off on the UAT obtained from OCAC. The implementation agency will have to facilitate the testing of all applications from OCAC users during the operational acceptance.

During the project, the Agency shall have coordination and full cooperation with the existing FMS service provider /vendor of OCAC. Since the project infrastructure has to be fully integrated with the OCAC IT Environment, the Implementation agency will require support from existing FMS and vice versa.

9.8 Project Planning & Management

The success of the project depends on proper project planning and management. At the onset, the Service Provider shall plan the project implementation in detail and should provide a micro-level view of the tasks and activities required to be undertaken in consultation with OCAC. The initial list of planning-related tasks and procedures (along with corresponding documentation) that the Service Provider should be submitted at the onset is as follows:

Project Schedule: A detailed day-wise timeline indicating various activities to be performed along with completion dates and resources required for the same

- i. Progress Monitoring Plan: Detailed Daily, Weekly, Monthly Progress Report formats along with

- ii. issue escalation format. The format shall be approved by Committee to the successful bidder before the start of the project.
- iii. Risk Mitigation Plan: List of all possible risks and methods to mitigate them.
- iv. Escalation Matrix & Incident Management: A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This must be in an Incident Management system.

DHCP setup

The DHCP HA cluster for Secretariat, SDC and SWAN will be on virtual/appliance servers and has provision to add more sites in the future.

DNS setup

The DNS HA cluster for Secretariat, SDC and SWAN will be on virtual/appliance-based servers and has provision to add more sites in the future.

The External DNS servers are setup with a hidden master (x.x.x.x) and two unicast secondaries in HA at DC & DR (x.x.x.x & x.x.x.x).

The Internal DNS servers are setup in HA at DC & DR for recursive lookup for entire campus ipv4 space. Internal DNS also acts as Authoritative DNS server for internal FQDN.

Internal DNS & External Authoritative DNS should be separated DNS servers & should not be DNS views based deployment.

Internal

Exposed to site/campus and wireless and contains internal-only data and email/admin contact information for all hosts. It is expected that this contact information will no longer be exposed via DNS, but through an API within the IPAM solution. Thus, the internal server should not be exposed off-site.

External

Exposed to public for secure access of hosted applications on SDC, Secretariat and SWAN.

General information to include:

- Performance measurement and reporting features for each of: DNS, DHCP, database, management interface
- Capacity measurement and reporting features for each of DNS, DHCP, database, management interface

- Scaling properties and limits (by IP address count, by DNS record count, transaction rate, by server type, administrative user count, by concurrent administrative user logins)
- Database backup and restore features
- Fault-tolerance features and options
- Features/options for managing overlapping IP address space (eg. multiple overlapping allocations of RFC 1918 space within the enterprise)
- Database and replication architecture
- Architecture of services (DNS/DHCP) integration with database.
- Describe any IPv6 features not supported or not at feature parity with IPv4
- DNS solution must support to integration with ArcSight SIEM and SOAR from day one.
- DNS solution must support detecting common webserver CVEs detect and block
- DNS firewall support to integrate other Intelligence feeds.
- The threat intelligence feeds should be available in multiple formats.
- Provide scripts-based threat intelligence feeds whenever required to download the data feeds.
- The solution should support Email and SMS notification integration.

9.9 Functional requirements

9.9.1 Implementation Plan

The proposed solution will run parallel with the existing system for two months as a transition. The production solution is based on products as described above. In responding to this RFP, please detailed the implementation plan that will systematically allow for this deployment and the associated downtime. After the needful transition downgrades of the existing setup, the whole environment will run stand on the new platform.

9.9.2 Required features

9.9.2.1 General Requirement

1. DDI System must be an Appliance/Virtual based solution providing all DNS, DHCP & IPAM with defined features & capacity from a single vendor.
2. DDI System must provide integrated support for high availability configurations without the requirement for licensing of additional third-party software components.

3. DDI System must support System logs forwarding/redirection of logs to a defined Syslog host.
4. DDI system must support monitoring using SNMPv2/3
5. DDI system must support NTP time synchronization (client mode) to multiple servers.
6. DDI system must integrate with multiple pass-through authentication options including RADIUS, LDAP, Active Directory
7. DDI Solution must support GUI & CLI-based configuration.
8. DDI Solution proposed should be deployed on-prem & should have the ability to host cloud/SAAS-based solution.

9.9.2.2 External DNS Server

1. Solution must support standards-based DNS services.
2. The solution must support the ability to act as an **External** Authoritative name server
3. Solution should support standards-based DNS services on-prem & should have the ability to host on a cloud-based Solution.
4. System proposed should be deployed 2 Qty at DC & 2 Qty at DR as a dedicated External Authoritative name server & 2 Qty of Hidden Master Server with 1 Qty at DC & 1 Qty at DR
5. The Solution must support **90,000 DNS QPS** acting as an internal DNS Server.
6. The Solution must support configuring 200 Zone & 1000 Records on a single instance.
7. The Solution must support Master-Slave, Multi-Master, or Stealth Mode deployment architecture.
8. Authoritative Name Servers must have built-in protection using Response Rate limiting
9. The solution must allow adding the following types of zones: Forward Mapping (Authoritative, Forward, Stub), Reverse Mapping (IPv4 and IPv6).
10. Authoritative Name Servers must have built-in protection using DNS DDoS protection - DNS Amplification/DNS reflection attacks.
11. The Solution must support A, NAPTR, SRV, NS, MX, CNAME records.
12. The Solution must support IPv6: AAAA, PTR, host, ip6.arpa, DDNS records.
13. The Solution must support multiple DNS views based on IPv4/IPv6 Addresses.
14. The Solution must support Instant propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc.

15. The solution must support easy search, sort and filter on any DNS Zone or RR, using any field
16. The product must support the ability to control DNS logging: DNS query and response logging
17. The solution must provide a simplified/streamlined process to identify and manage DKIM, DMARC, ADSP, SPF and/or other similar DNS TXT records.
18. The system must be able to display all hosted DNS Resource Records in one GUI pane.
19. The solution must support the standard DNSSEC specifications for serving of DNSSEC-signed zones and the pass-through of client resolution of external zones.
20. The proposed solution MUST support DNS Security features to protect DOS, DNS Exploits, DNS Amplification and Reflection Attacks, DNS UDP Flood Attack, Spoofed Source Address Attack, Protocol anomalies.
21. The proposed solution must provide updates to the security protection rules
22. Solution shall use technology to automatically update protection against new and evolving threats as they emerge to protect DNS service
23. The solution must have inbuilt reports & Status.
24. The solution should be flexible for global application management in virtual and multi-cloud environments. The web-based UI provides easy DNS configuration with centralized menus; advanced logging, statistics, and reporting along with export to 3rd party analytics.
25. Ensure DNS and application availability and protection during DNS DDoS attacks or volume spikes. Mitigate DNS threats by blocking access to malicious IP domains based on reputational feeds.

9.9.2.3 Internal DNS

1. The Solution must support **75,000** QPS internal DNS servers.
2. System should have a Cache & Internal Authoritative DNS Functionality.
3. Solution should support standards-based DNS services on-prem & should not be a cloud-based Solution.
4. System proposed should be deployed 2 Qty at DC & 2 Qty at DR.
5. System should have a Cache DNS architecture to switch on demand from BIND to UNBOUND and vice versa.
6. System should be able to support the following common resource record types of namely A, AAAA, DNAME, CNAME, MX, HINFO, PTR, SOA, and NX.

7. System should be deployed on-premises.
8. System should regularly monitor its cache contents and automatically purge/remove records that are old.
9. System should have a built-in RPZ functionality and not require additional licenses to enable such a feature.
10. The vendor must have his own Threat Intelligence unit.
11. The solutions must be able to deliver contextual awareness service and analysis to block threats from a dynamic set of high-risk IP addresses, to Detect malicious activities and sites and IP addresses
12. DNS firewall and DNS malware prevention must work on all DNS query types such as A, AAAA, NS, SOA, MX, CNAME, ANY, PTR etc.
13. OEM must-have tool/third-party feeds that security analysts can use to report on why domains were classified as malicious by the DNSFW/threat feed (Threat Lookup)
14. The behavior engine shall detect the DNS tunneling, anomaly and DNS exfiltration/infiltration automatically and once detected automatically apply policy using RPZ to block the communication
15. The vendor shall have an in-house threat research team to provide real-time intelligence and depend on third-party feeds to enrich the threat feeds.
16. The Proposed Recursive DNS should have the capability to secure from the below attacks.
 - a. DNS Data Exfiltration
 - b. Volumetric NXDomain DoS attacks
 - c. Phantom domain attacks
 - d. BIND Zero-day vulnerability attacks
 - e. DNS cache poisoning attacks
 - f. DNS Amplification and Reflection Attacks
 - g. Resource Utilization Attacks
 - h. Domain lock-up attacks
 - i. Basic NXDOMAIN attack
 - j. Random subdomain attack
 - k. DNS Domain-based protection
 - l. DNS Sloth Attack
 - m. Recursive layer attack
17. The Solution should be able to protect the Cache DNS Servers or freeze the DNS Cache content in the event of receiving a DDOS Attack even when the source of the attack cannot be identified.

18. The Solution should have the ability to Log Only, Quarantine or Block poorly behaving clients based on their DNS Transactions.
19. The Solution should provide for DNS Cache Saving to retain Cache Data even while applying software updates, patches, upgrades and reboot.
20. The Solution should have the ability to identify the poorly behaving clients based on their DNS Transactions & only allow client to access DNS Cache entries.
21. The Solution should have the ability to identify the poorly behaving clients based to allow clients to access Cache & restrict recursive query which seems to exfiltrate the using DNS protocol.
22. System solution should be able to support RPZ feeds to protect from Anti-Malware, Anti-phishing, Anti-spam, and Cracked Website.
23. System RPZ should support action as Block, walled redirection, no response.
24. System should support Access Control based on Source IP for Allow Query, Allow Query Cache.
25. System should Support DNSSEC.
26. System must support Anycast for DNS with BGP, IS-IS and OSPF.
27. System should support an audit log.
28. System should support granular rights administration limiting the function and rights to user and zone levels.
29. System should support sending logs to SIEM and the external Syslog server

9.9.2.4 DHCP

1. The solution must provide an easy-to-use "import wizard" to import DHCP records from the legacy DHCP Solution.
2. Import Wizard solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines.
3. The DHCP solution must provide high availability across two (2) data centers.
4. Proposed DHCP solution should be deployed 1 Qty at DC & 1 Qty at DR
5. The solution must track and log all user changes to DHCP configurations. The audit logs must be able to identify the change(s) made, the user/system making

the change, and a timestamp. The solution should also be able to identify the client's IP address from where the change was made.

6. The solution must be able to handle **450 DHCP** Lease/sec.
7. The solution must be able to perform Dynamic DNS for both IPv4 and IPv6 while linking all associated IP addresses to a single device/object.
8. The solution must graph (visually display) the different scopes based on the number of IPs used/available over a set period.
9. The DHCP solution must support one IP per MAC address (one lease per client).
10. The DHCP solution must be able to release the DHCP lease if the MAC address has moved to another IP.
11. The solution must provide device fingerprinting and display or report the data in the GUI.
12. The solution must support creating DHCP custom options.
13. The solution must provide the ability to detect or block devices attempting to use DHCP based on various attributes. These attributes must include MAC address but can include device fingerprint, DHCP options, etc.
14. The DHCP Solution must integrate into IPAM for lease consolidation and capacity planning.
15. The DHCP Solution must have its built-in security mechanism against Rogue Clients performing DHCP Storm attacks without the need for additional licenses.
16. The DHCP Solution must be able to send alerts in case of DHCP-related attacks.
17. The DHCP Solution must have inbuilt Reports & statuses.

9.9.2.5 IPAM

1. The IPAM Solution must support **300,000** IP Address Management for both IPv4 & IPv6 together.
2. The solution must NOT use software agents or thick clients
3. The IPAM solution must provide high availability across DC & DR
4. System proposed should be deployed 1 Qty at DC & 1 Qty at DR.
5. The solution should provide appropriate automated failover between the data center and the disaster recovery center. The database Synchronization between DC & DR should be automatic.
6. The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI.

7. The solution must include an application programming interface (API) in order to interface with the network and/or asset management systems, a configuration management database (CMDB) solution or other applications.
8. The IPAM solution should be able to seamlessly integrate with DNS and DHCP Records
9. The IPAM solution should be able to create its own widget to display customized subnet reports, free IP, used IP.
10. The IPAM solution should have the ability to locate the available subnets inside a Supernet. This is to provide assistance to users when creating subnets inside an aggregated Network.
11. DDI IPAM user interface must be web-based without specific browser vendor requirements
12. DDI IPAM system should support seamless failover between DC and DR
13. DDI IPAM system should support VLSM (Variable Length Subnet Masks)
14. DDI IPAM system should be able to export reports in PDF, CSV format
15. DDI IPAM system should have support for workflow processes for various administrator roles and should include a change approval oversight capability.
16. DDI audit records should contain a timestamp, username and record modified.
17. DDI Reporting engine should include audit reports.

9.10 Technical Support

- The bidder must provide required support to OCAC after installation and commissioning.
- The bidder (through OEM) must provide training to the selected professionals of OCAC on the quoted products and management.
- Bidder is also allowed to conduct training session in VC mode.
- The bidder must engage a OEM Certified support staff for a initial period of 2 years at OCAC. However, the period of engagement shall be increased depending upon the requirements at the same pricing term.
- The support person/ team shall remain readily available to the OCAC support team on phone/ email and shall be readily available in person to the premises when required. However, if required, OCAC/Govt. may ask the bidder's support person/ team to be available on holidays/ beyond office hours. The bidder shall be required to immediately provide a replacement support person; in case the deputed person is on leave due to any reasons.

9.11 Specification and features

DDI Appliances with Licenses

Make: (Bidder to Specify)

Model: (Bidder to Specify)

Licenses		
Minimum Subscription Description (External DNS Server)	Compliance (Yes/No)	Cross Reference
The solution must support standards-based DNS services.		
The solution must support the ability to act as an External Authoritative name server		
The solution should support standards-based DNS services on-prem & should not be cloud-based Solution.		
The system proposed should be deployed 2 Qty at DC & 2 Qty at DR as a dedicated External Authoritative name server & 2 Qty of Hidden Master Server with 1 Qty at DC & 1 Qty at DR		
The Solution must support 90,000 DNS QPS acting as an internal DNS Server.		
The Solution must support configuring 200 Zone & 1000 Records on a single instance.		
The Solution must support Master-Slave, Multi-Master or Stealth Mode deployment architecture.		
Authoritative Name Servers must have built-in protection using Response Rate limiting		
The solution must allow adding the following types of zones: Forward Mapping (Authoritative, Forward, Stub), Reverse Mapping (IPv4 and IPv6).		
Authoritative Name Servers must have built-in protection using DNS DDoS protection - DNS Amplification/DNS reflection attacks.		
The Solution must support A, NAPTR, SRV, NS, MX, CNAME records.		
The Solution must support IPv6: AAAA, PTR, host, ip6.arpa, DDNS records.		
The Solution must support multiple DNS views based on IPv4/Ipv6 Addresses.		

The Solution must support Instant propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc.		
The solution must support easy search, sort and filtering on any DNS Zone or RR, using any field		
The product must support the ability to control DNS logging: DNS query and response logging		
The solution must provide a simplified/streamlined process to identify and manage DKIM, DMARC, ADSP, SPF and/or other similar DNS TXT records.		
The system must be able to display all hosted DNS Resource Records in one GUI pane.		
The solution must support the standard DNSSEC specifications for serving of DNSSEC-signed zones and the pass-through of client resolution of external zones.		
The proposed solution MUST support DNS Security features to protect against DOS, DNS Exploits, DNS Amplification and Reflection Attacks, DNS UDP Flood Attacks, Spoofed Source Address Attacks and Protocol anomalies.		
The solution must have inbuilt reports & Status.		
The solution must provide signature-based, reputational-based, and behavioral-based security measures		
The proposed solution must provide updates to the security protection rules		
The solution shall use technology to automatically update protection against new and evolving threats as they emerge to protect the DNS service		
The solution shall use technology to automatically update protection against new and evolving threats as they emerge to protect the DNS service		
The solution should be flexible for global application management in virtual and multi-cloud environments. The web-based UI provides easy DNS configuration with centralized menus; advanced logging, statistics, and reporting along with export to 3rd party analytics.		
Ensure DNS and application availability and protection during DNS DDoS attacks or volume spikes. Mitigate DNS threats by blocking access to malicious IP domains based on reputational feeds.		

Minimum Subscription Description (Internal DNS Server)	Compliance (Yes/No)	Cross Reference
The Solution must support 75,000 QPS internal DNS servers.		
The system should have a Cache & Internal Authoritative DNS Functionality.		
The system proposed should be deployed 2 Qty at DC & 2 Qty at DR.		
The system should have a Cache DNS architecture to switch on demand from BIND to UNBOUND and vice versa.		
The system should be able to support the following common resource record types namely A, AAAA, DNAME, CNAME, MX, HINFO, PTR, SOA, and NX.		
The system should be deployed on-premise.		
The system should regularly monitor its cache contents and automatically purge/remove records that are old.		
The system should have a built-in RPZ functionality and not require additional licenses to enable such a feature.		
The vendor must have his own Threat Intelligence unit.		
The solutions must be able to deliver contextual awareness service and analysis to block threats from a dynamic set of high-risk IP addresses and to Detect malicious activities and sites and IP addresses.		
DNS firewall and DNS malware prevention must work on all DNS query types such as A, AAAA, NS, SOA, MX, CNAME, ANY, PTR etc.		
<p>OEM must-have tool/third-party feeds that security analysts can use to report on why domains were classified as malicious by the DNSFW/threat feed (Threat Lookup)</p> <p>The behaviour engine shall detect the DNS tunnelling, anomaly and DNS exfiltration/infiltration automatically and once detected automatically apply policy using RPZ to block the communication.</p>		
System should Support DNSSEC.		
The vendor shall have an in-house threat research team to provide real-time intelligence and depend on third-party feeds to enrich the threat feeds.		

<p>The Proposed Recursive DNS should have the capability to secure from below attacks.</p> <ul style="list-style-type: none"> a. DNS Data Exfiltration c. Volumetric NXDomain DoS attacks c. Phantom domain attacks d. BIND Zero-day vulnerability attacks e. DNS cache poisoning attacks f. DNS Amplification and Reflection Attacks g. Resource Utilization Attacks h. Domain lock-up attacks i. Basic NXDOMAIN attack j. Random subdomain attack k. DNS Domain-based protection l. DNS Sloth Attack m. Recursive layer attack 		
<p>The Solution should be able to protect the Cache DNS Servers or freeze the DNS Cache content in the event of receiving a DDOS Attack even when the source of the attack cannot be identified.</p>		
<p>The Solution should have the ability to Log Only, Quarantine or Block poorly behaving clients based on their DNS Transactions</p>		
<p>The Solution should provide for DNS Cache Saving to retain Cache Data even while applying software updates, patches, upgrades and reboot.</p>		
<p>The Solution should have the ability to identify the poorly behaving clients based on their DNS Transactions & only allow clients to access DNS Cache entries.</p>		
<p>The Solution should have the ability to identify the poorly behaving clients based to allow clients to access Cache & restrict recursive queries which seem to exfiltrate the using DNS protocol.</p>		
<p>The system solution should be able to support RPZ feeds to protect from Anti-Malware, Antiphishing, Anti-spam, and Cracked websites.</p>		
<p>System RPZ should support action as Block, walled redirection, no response.</p>		

The system should support Access Control based on Source IP for Allow Query and Allow Query Cache.		
The system should support an audit log.		
The system should support granular rights administration limiting the function and rights to user and record levels.		
The system should support sending logs to SIEM and the external Syslog server		
Minimum Subscription Description (DHCP Server)	Compliance (Yes/No)	Cross Reference
The solution must provide an easy-to-use "import wizard" to import DHCP records from the legacy DHCP Solution.		
Import Wizard solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines.		
The DHCP solution must provide high availability across two (2) data centers.		
The proposed DHCP solution should be deployed 1 Qty at DC & 1 Qty at DR		
The solution must track and log all user changes to DHCP configurations. The audit logs must be able to identify the change(s) made, the user/system making the change, and a timestamp. The solution should also be able to identify the client's IP address from where the change was made.		
The solution must be able to handle 450 DHCP Lease/sec .		
The solution must be able to perform Dynamic DNS for both IPv4 and IPv6 while linking all associated IP addresses to a single device/object.		
The solution must graph (visually display) the different scopes based on the number of IPs used/available over a set period of time.		
The DHCP solution must support one IP per MAC address (one lease per client).		
The DHCP solution must be able to release the DHCP lease if the MAC address has moved to another IP.		
The solution must provide device fingerprinting and display or report the data in the GUI.		
The solution must support creating DHCP custom options.		

The solution must provide the ability to detect or block devices attempting to use DHCP based on various attributes. These attributes must include MAC address but can include device fingerprint, DHCP options, etc.		
The DHCP Solution must integrate into IPAM for lease consolidation and capacity planning.		
The DHCP Solution must have its built-in security mechanism against Rogue Clients performing DHCP Storm attacks without the need for additional licenses.		
The DHCP Solution must be able to send alerts in case of DHCP-related attacks.		
The DHCP Solution must have inbuilt Reports & statuses.		
Minimum Subscription Description (IPAM)	Compliance (Yes/No)	Cross Reference
The IPAM Solution must support 300,000 IP Address Management for both IPv4 & IPv6 together.		
The solution must NOT use software agents or thin clients		
The IPAM solution must provide high availability across DC & DR		
The proposed DHCP solution should be deployed 1 Qty at DC & 1 Qty at DR		
The solution should provide appropriate automated failover between data center and the disaster recovery center. The database Synchronization between DC & DR should be automatic.		
The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI.		
The solution must include an application programming interface (API) in order to interface with network and/or asset management systems, a configuration management database (CMDB) solution or other applications.		
The IPAM solution should be able to seamlessly integrate with DNS and DHCP Records		
The IPAM solution should be able to create its own widget to display customized subnet reports, free IP and used IP.		
The IPAM solution should have the ability to locate the available subnets inside a Supernet. This is to provide		

assistance to users when creating subnets inside an aggregated Network.		
DDI IPAM user interface must be web-based without specific browser vendor requirements		
DDI IPAM system should support seamless failover between DC and DR		
DDI IPAM system should support VLSM (Variable Length Subnet Masks)		
DDI IPAM system should be able to export reports in PDF, CSV format		
DDI IPAM system should have support for workflow processes for various administrator roles and should include a change approval oversight capability.		
DDI audit records should contain a timestamp, username and record modified.		
The DDI Reporting engine should include audit reports.		

9.12 Bill of Materials

Sl. No.	Description	Qty	Unit
1	Appliance (External DNS) with Security (along with 1 st year warranty and subscription)	2	Nos
2	Appliance (Internal DNS) with Security (along with 1 st year warranty and subscription)	2	Nos
3	DHCP and IPAM License (along with 1 st year support and subscription)	2	Nos
4	Central Management (along with 1 st year support and subscription)	2	Nos
5	Reporting and Analytics (along with 1 st year support and subscription)	2	Nos
6	Warranty support along with subscription of required Licenses for additional 4 Years after 2 nd Year onwards up to 5 th Year against above appliances and licenses	4	Years
7	Deployment of one OEM certified Support staff (initially for 24 months which may be extended further depending upon requirement)	24	Months
7	Installation and Commissioning	1	Lumpsum
8	OEM training for selected professionals of OCAC	20	officials

9.13 Contract Period

Then engagement of the service provider shall be for a period of 5 years from the date of commencement service i.e. date of commissioning.

9.14 Timeline and Penalty

9.14.1 Delivery, Installation and Commissioning

Requirement	Timeline	Penalty
Supply of material (both appliances and software licenses)	Within 12 weeks from the issue of work order	0.5% per week against the un-delivered material cost
Installation and commissioning	Within 4 weeks from the date of supply of materials	0.5% per week against the Installation and Commissioning cost
Deployment of support staff	Within 4 weeks from installation and commissioning	1% per week against monthly manpower cost
Replacement of support staff	Within 2 weeks from resignation of existing support staff/instructions from OCAC on replacement of staff	1% per week against monthly manpower cost

9.14.2 Penalty for Non-Availability/Downtime of Service

Level of availability calculated on monthly basis	Penalty Amount
> 99% or more	No penalty would be deducted
>=98% and < 99%	2% of amount payable
>=96% and < 98%	5% of amount payable
>=95% and < 96%	7% of amount payable
< 95%	10% of amount payable

Penalty for non-availability/downtime of service shall be applicable on the total quarterly usage billed amount the respective quarter which the downtime has been recorded for.

9.14.3 Other Penalty terms

- a. The maximum total penalty in any quarter shall not be more than 10% of the total amount due for the quarter.

- b. Penalty of 10% for consecutive two quarters may be treated as breach of contract and OCAC may take suitable actions accordingly.
- c. Maximum penalty shall not be more than 10% of the total due.
- d. Payment shall not be imposed, if the cause of delay/non delivery service is not attributable to bidder.

9.15 Payment term

9.15.1 Appliance Cost

- a. 60% of the appliance cost shall be paid after delivery of the material and inspection thereof.
- b. 20% of the appliance cost shall be paid after Installation and commissioning.
- c. Balance 20% of the appliance cost shall be paid after successful running of the appliances for a period of three months. This payment shall be made after deduction of Penalty for Non-Availability/Downtime of Service as described in clause 9.14.2, if any.

9.15.2 License Cost

100% of the license cost shall be paid after Installation and commissioning.

9.15.3 Installation and Commissioning

- a. 70% of the installation and commissioning cost shall be paid after Installation and commissioning.
- b. Balance 30% of the installation and commissioning shall be paid after successful running of the appliances and software for a period of three months.

9.15.4 Warranty support and subscription cost

- a. 100% of the yearly cost against warranty support and subscription (as mentioned at Clause no. 9.12 Bill of materials SL# 6) shall be released beginning of the respective year w.r.t date of commissioning.
- b. This payment shall be made after deduction of Penalty for Non-Availability/Downtime of Service as described in clause 9.14.2 for the previous year, if any.

9.15.5 Support Resource cost

- c. 100% of the payment towards cost of manpower resource shall be paid quarterly basis.

10 Formats for Response

10.1 Pre-Qualification Bid Formats

10.1.1 FORM PQ-1: Cover Letter

(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.

Sub: RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha

Ref: RFP Reference No. -OCAC-SEGP-INFRA-0002-2019-ENQ-23013

Madam,

I, the undersigned, offer to provide the services for the proposed assignment in respect to your Request for Proposal No. -OCAC-SEGP-INFRA-0002-2019-ENQ-23013. We hereby submit our proposal which includes the pre-qualification proposal, technical proposal and commercial proposal, sealed under separate envelopes. Our proposal will be valid for acceptance up to 120 Days and I confirm that this proposal will remain binding upon us and may be accepted by you at any time before this expiry date.

All the information and statements made in our proposal are true and correct and I accept that any misinterpretation contained in it may lead to disqualification of our proposal. If negotiations are held during the period of validity of the proposal, I undertake to negotiate on the basis of proposal submitted by us. Our proposal is binding upon us and subject to the modifications resulting from contract negotiations.

I have examined all the information as provided in your Request for Proposal (RFP) and offer to undertake the service described in accordance with the conditions and requirements of the selection process. I agree to bear all costs incurred by us in connection with the preparation and submission of this proposal and to bear any further pre-contract costs. In case, any provisions of this RFP/ ToR/Scope including of our technical and financial proposal are found to be deviated, then you shall have rights to reject our proposal. I confirm that, I have the authority to submit the proposal and to clarify any details on its behalf.

I understand you are not bound to accept any proposal you receive.

Yours faithfully,

(Authorized Signatory)
Name, Designation & Contact No.
Seal

10.1.2 FORM PQ-2: Bidder's Organization (General Details)

(To be submitted on the Letterhead of Bidder)

Sl#	Information	Details
1.	Name of Bidder	
2.	Registered Address of Bidder	
3.	Address for Communication	
4.	Address of local office in Odisha.	
5.	Name, Designation and Address of the contact person to whom all references shall be made regarding this RFP	
6.	Mobile no. of contact person:	
7.	E-mail address of contact person:	
8.	GST Number of the Firm	
9.	PAN No. of the firm	

Yours faithfully,

(Authorized Signatory)
Name, Designation & Contact No.
Seal

10.1.3 FORM PQ-3 [Acceptance of Terms and Conditions]

(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.

Sub: RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha

Madam/Sir,

I have carefully and thoroughly gone through the Terms & Conditions along with scope of work contained in the RFP No. -OCAC-SEGP-INFRA-0002-2019-ENQ-23013 regarding RFP for "Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha".

I declare that all the provisions/clauses including scope of work of this RFP are acceptable to our company. I further certify that I am an authorized signatory of the company and I am, therefore, competent to make this declaration.

Yours faithfully,

(Authorized Signatory)
Name, Designation & Contact No.
Seal

10.1.4 FORM PQ-4 [Self-Declaration against Not-Blacklisted]

(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.

Sub: RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha

Ref : RFP Ref No. -OCAC-SEGP-INFRA-0002-2019-ENQ-23013

Sir

In response to the RFP No.: -OCAC-SEGP-INFRA-0002-2019-ENQ-23013 for RFP titled "RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha", as an owner/ partner/ Director of (organisation 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.

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,

Yours faithfully,

(Authorized Signatory)

Name, Designation & Contact No.

Seal

10.1.5 FORM PQ-5: Project Citation Format

a)	Project Name:	
b)	Value of Contract/ Work Order (In INR):	
c)	Name of the Client:	
d)	Project Location:	
e)	Contact person of the client with address, phone and e-mail:	
f)	Project Duration:	
g)	Start Date (month/year): Completion Date (month/year):	
h)	Status of assignment: Completed / Ongoing (if it is on-going, level of completion)	
i)	Narrative description of the project with scope:	
j)	List of Services provided by your firm/company:	

10.1.6 FORM PQ-6: Bidder's Authorization Certificate

To (Company letter head)
The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of E&IT Dept, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL, Bhubaneswar - 751013

Sub: RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha– Bidder's Authorization Certificate

Sir,

With reference to the RFP No.: -OCAC-SEGP-INFRA-0002-2019-ENQ-23013, Ms./Mr. <Name>, <Designation> is hereby authorized to attend meetings & submit pre-qualification, technical & commercial information as may be required by you in the course of processing the above said Bid. S/he is also authorized to attend meetings & submit technical & commercial information as may be required by you in the course of processing above said application. Her/his contact mobile number is _____ and Email id is _____. For the purpose of validation, his/ her verified signatures are as under.

Thanking you,

Signature
(Authorised Signatory)

Verified Signature by
Director/CEO

Seal:

Date:

Place:

Name of the Bidder:

10.1.7 Format for Bank Guarantee for Earnest Money Deposit

To

The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of E&IT Dept, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL, Bhubaneswar - 751013

Sub: RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha

RFP No.: -OCAC-SEGP-INFRA-0002-2019-ENQ-23013

Whereas <<Name of the bidder>> (hereinafter called 'the Bidder') has submitted the bid for Submission of RFP Ref. No. -OCAC-SEGP-INFRA-0002-2019-ENQ-23013, for engagement of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha (hereinafter called "the Bid") to OCAC.

Know all Men by these presents that we <<Name of the Bidder>> having our office at <<Address>> (hereinafter called "the Bank") are bound unto the Odisha Computer Application Centre (hereinafter called "the Purchaser") in the sum of Rs. 20,00,000/- (Rupees Fifteen Lakh only) for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents.

Sealed with the Common Seal of the said Bank this <<Date>>

The conditions of this obligation are:

1. If the Bidder withdraws or amends, impairs or derogates from the tender in any respect within the period of validity of this tender; or
2. If the Bidder have been notified of the acceptance of his tender by the Purchaser during the period of its validity :-
 - a. If the tenderer fails to furnish the Performance Security for the due performance of the contract; or
 - b. Fails or refuses to accept/execute the contract;

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

This guarantee will remain in force up to <<insert date>> and including <<extra time over and above mandated in the RFP>> from the last date of submission and any demand in respect thereof should reach the Bank not later than the above date.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN:

- i) Our liability under this Bank Guarantee shall not exceed Rs. <<Amount in figures>> (Rupees <<Amount in words>> only)
- ii) This Bank Guarantee shall be valid upto <<insert date>>)
- iii) It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before <<insert date>>) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

Seal:

Date:

10.2 Technical Bid Formats

10.2.1 FORM TECH-1: Description of Proposed Solution along with Technology, Scalability, Completeness and compliance details as per the specification

Bidder has to provide details of the entire solution proposed covering all requirements as listed out in this RFP.

Bidder has to specifically include (but not limited to) diagram and detailed description of the following:

- a) Functional Architecture
- b) Technical Architecture
- c) Network Architecture
- d) Deployment Architecture
- e) Security Architecture

Bidder must cover all aspects of the solution while showcasing its scalability, completeness, simplicity and interoperability.

- Bidder must submit the required documents against compliance to the scope of work.
- Bidder is free to propose any type of approach for implementation of the assignment

10.2.2 FORM TECH-3: Detailed Work Plan with Activities, Duration, Sequencing, Interrelations, Milestones and Dependencies

SL#	Deliverable/ Activity*	Months							
		1	2	3	4	5	6	7	n
a)									
b)									
c)									
d)									
e)									
f)									
g)									
h)									
i)									
j)									
k)									
l)									
m)									
n)									
o)									
p)									
q)									
r)									
s)									

10.2.3 FORM TECH-4: Support Structure

Bidder to specify the support structure.

10.3 Financial Bid

10.3.1 FORM FIN-1: Financial Bid Covering Letter

(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.

Sub: RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha

Ref: RFP Reference No. -OCAC-SEGP-INFRA-0002-2019-ENQ-23013

Madam/Sir,

I /We, the undersigned, offer to provide the service for provision of DNS-DHCP-IPAM Solutions for Govt. of Odish as per RFP No.: -OCAC-SEGP-INFRA-0002-2019-ENQ-23013 and our Pre-Qualification, Technical and Financial Proposals. Our attached Financial Proposal is for the sum of <<Amount in words and figures>> inclusive of all applicable taxes and duties.

a) BID PRICE

We declare that our Bid Price is for the entire scope of the work as specified in this RFP. These prices are indicated in the Financial Bid as part of this RFP response. In case there is substantial difference between the component wise price approved by OCAC and the price quoted by the bidder, OCAC will have the rights to ask the bidder to realign their prices without impacting the total bid price. We hereby agree to submit our offer accordingly.

b) PRICE AND VALIDITY

All the prices mentioned in our Tender are in accordance with the terms as specified in the RFP documents. All the prices and other terms and conditions of this Bid are valid for a period of 5 years from the date of opening of the Bid.

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.

c) 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.

d) TENDER PRICING

We further confirm that the prices stated in our bid are in accordance with your clauses in RFP/Tender document.

e) QUALIFYING DATA

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

f) PERFORMANCE BANK GUARANTEE

We hereby declare that in case the contract is awarded to us, we shall submit the Performance Bank Guarantee as specified in this RFP document.

We understand you are not bound to accept any Proposal you receive. We hereby declare that our Proposal is made in good faith, without collusion or fraud and the information contained in the proposal is true and correct to the best of our knowledge and belief.

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

Yours faithfully,

(Authorized Signatory)
Name, Designation & Contact No.
Seal

10.3.2 Commercial bid

Sl#	Category	Quantity (Indicative)	Unit	Unit Cost (excluding GST)	Total cost (excluding GST)
A	B	C	D	E	F (C * E)
1.	Appliance (External DNS) with Security (along with 1 st year warranty and subscription)	2	Nos		
2.	Appliance (Internal DNS) with Security (along with 1 st year warranty and subscription)	2	Nos		
3.	DHCP and IPAM License (along with 1 st year support and subscription)	2	Nos		
4.	Central Management (along with 1 st year support and subscription)	2	Nos		
5.	Reporting and Analytics (along with 1 st year support and subscription)	2	Nos		
6.	Warranty support along with subscription of required Licenses for additional 4 Years after 2 nd Year onwards up to 5 th Year against above appliances and licenses	4	Years		
7.	Deployment of one OEM certified Support staff (initially for 24 months which may be extended further depending upon requirement)	24	Months		
8.	Installation and Commissioning	1	Lumpsum		
9.	OEM training for selected professionals of OCAC	20	officials		
10.	Any other cost, bidder may specify				
Grand Total (Excluding GST)					

Sl#	Category	Quantity (Indicative)	Unit	Unit Cost (excluding GST)	Total cost (excluding GST)
A	B	C	D	E	F (C * E)
Grand Total in words					

(GST shall be applicable as per actual at the time of billing)

- The Bidder, who has submitted the lowest Commercial bid (i.e. lowest in Grand Total) , shall be selected as the L1 and shall be called for further process leading to the award of the assignment.
- The bid price will be exclusive of all taxes and levies and shall be in Indian Rupees.
- Errors & Rectification: Arithmetical errors will be rectified on the following basis: “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. If there is a discrepancy between words and figures, the amount in words will prevail”.

10.3.3 Performance Security

To

The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of E&IT Dept, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL, Bhubaneswar - 751013

Sub: RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha

RFP No.: -OCAC-SEGP-INFRA-0002-2019-ENQ-23013

Whereas, <<name of the supplier and address>> (hereinafter called “the bidder”) has undertaken, in pursuance of contract no. <Insert Contract No.> dated. <Date> to provide DNS-DHCP-IPAM Solution for Govt. of Odisha (hereinafter called “the beneficiary”)

And whereas it has been stipulated by in the agreement that the bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the agreement;

And whereas we, <Name of Bank> a banking company incorporated and having its head /registered office at <Address of Registered Office> and having one of its office at <Address of Local Office> have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of <<Cost of Service>> in (words) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the agreement and without cavil or argument, any sum or sums within the limits of <<Cost of Service>> (in Words) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the agreement to be performed there under or of any of the agreement documents which may be made between you and the Bidder shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification. This Guarantee shall be valid until <<<insert date>>

Notwithstanding anything contrary contained in any law for the time being in force or banking practice, this guarantee shall not be assignable or transferable by the

beneficiary i.e OCAC. Notice or invocation by any person such as assignee, transferee or agent of beneficiary shall not be entertained by the Bank.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN:

- i) Our liability under this bank guarantee shall not exceed <<amount>> (Amt. in words).
- ii) This bank guarantee shall be valid up to <<insert date>>.
- iii) It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before <<insert date>> failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

Seal:

Date:

11 Proposed Master Service Agreement

Master Service Agreement for engagement of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha

This agreement is made on ____/____/____ between Odisha Computer Application Centre, the Designated Technical Directorate of Electronics and Information Technology Department, Government of Odisha having its office at Plot-N-1/7-D, Po- RRL, Acharya Vihar Square, Bhubaneswar - 751013, Odisha. (hereinafter called "**Purchaser**" or "**OCAC**") which expression shall unless repugnant to the context thereof include his successors, heirs, assigns, administrator, executive & representative of the one part,

And

M/s _____, a company registered under the Provisions of Act,1956 _____ is having its registered office at _____ India (hereinafter called "**Solution Provider**") which expression shall unless repugnant to the context thereof include his successors, heirs, assigns, administrator, executive and representatives of the other part.

WHEREAS OCAC had invited Request for Proposal (RFP) for engagement of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha)vide RFP Reference No. _____. Based on the tender evaluation, M/s _____ has been selected as "**Solution Provider**".

And in "pursuance of above facts the parties have agreed to enter into this agreement.

NOW THIS AGREEMENT WITNESSES AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Contract referred to.
2. The following documents (collectively referred to as "Contract Documents") shall be deemed to form and be read and construed as part of this Agreement, viz.:
 - a) RFP floated by OCAC Reference No. _____, Technical bid and Commercial furnished by Solution Provider with respect to RFP
 - b) The General Conditions of Contract
 - c) The Special Conditions of Contract
 - i) Following Appendix to GC and SC:
 - ii) Appendix-A: Scope of Work
 - iii) Appendix-B: Deliverables
 - iv) Appendix-C: Cost of Service

d) The mutual rights and obligations of the Purchaser and the Solution Provider shall carry out the Services in accordance with the provisions of the Contract;

IN WITNESS WHEREOF, the Parties hereto have caused this Contract to be signed in their respective names as of the day and year above written.

On behalf of Purchaser

On behalf of Solution Provider

Signature:
Name:
Designation:

Signature:
Name:
Designation:

Witness -1
Name & Address:

Witness -1
Name & Address:

Witness -2
Name & Address:

Witness -2
Name & Address:

1. GENERAL CONDITIONS OF CONTRACT

1.1. Definitions

Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings:

- 1.1.1. "Applicable Law" means the laws and any other instruments having the force of law in India.
- 1.1.2. "Bidder" means the entity bidding for the services under the Contract.
- 1.1.3. "Solution Provider" means M/s _____ whose proposal to perform the Contract has been accepted by the Purchaser and is named as such in the Agreement and may provide or provides the Services to the Purchaser under this Contract.
- 1.1.4. "Contract" means the Agreement entered into between the Purchaser and the Solution Provider, together with the contract documents referred to therein, including General Conditions (GC), the Special Conditions (SC), all the attachments, appendices, annexure, and all documents incorporated by reference therein.
- 1.1.5. "Deliverables" means the services agreed to be delivered by Solution Provider in pursuance of the agreement as defined more elaborately in the RFP;
- 1.1.6. "Effective Date" means the date on which this Contract comes into force i.e. Date of issuance of Purchase Order (referred as PO).
- 1.1.7. "Day" means a Govt. of Odisha working day.
- 1.1.8. "GC" mean these General Conditions of Contract.
- 1.1.9. "Government" means the Government of Odisha
- 1.1.10. "In writing" means communicated in written form with proof of receipt.
- 1.1.11. "Intellectual Property Rights" means any patents, copyrights, trademarks, trade names, industrial design, trade secret, permit, service marks, brands, proprietary information, knowledge, technology, licenses, databases, software, know-how, or other form of intellectual property rights, title, benefits or interest, whether arising before or after execution of the Contract.
- 1.1.12. "Member" means any of the entities that make up the joint venture / consortium / association, and "Members" means all these entities.
- 1.1.13. "Man-Month" means one resource working for 1 month (Calendar working days as per Govt. of Odisha).
- 1.1.14. "Party" means the Purchaser or the Solution Provider, as the case may be, and "Parties" means both of them.

- 1.1.15. "Personnel" means persons hired or appointed by the Solution Provider and assigned to the performance of the Services or any part thereof
- 1.1.16. "Purchaser" means Odisha Computer Application Centre, Designated Technical Directorate of Information Technology Department, Government of Odisha an entity purchasing the services under this Contract.
- 1.1.17. "Resident" means normal resident of Odisha
- 1.1.18. "RFP" means Request for Proposal invited for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha vide RFP Reference No.: OCAC-SEGP-INFRA-0002-2019-ENQ-23013.
- 1.1.19. "SC" means the Special Conditions of Contract by which the GC may be amended or supplemented.
- 1.1.20. "Services" means the work to be performed by the Solution Provider pursuant to this Contract, as described in Appendix-A hereto.
- 1.1.21. The "Selected Agency" means Agency which is selected through the tender process i.e. System Integrator / Solution Provider.
- 1.1.22. The "Service Provider (SP)" means service Provider engaged for the messaging service

1.2. Interpretation

In this Agreement, unless otherwise specified:

- 1.2.1. References to Clauses, Sub-Clauses, Paragraphs, Schedules and Annexures are to clauses, sub-clauses, paragraphs, schedules and annexures to this Agreement;
- 1.2.2. Use of any gender includes the other genders;
- 1.2.3. A reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted;
- 1.2.4. Any reference to a 'day' (including within the phrase 'business day') shall mean a period of 24 hours running from midnight to midnight;
- 1.2.5. References to a 'business day' shall be construed as a reference to Govt. of Odisha Working Day
- 1.2.6. References to times are to Indian Standard Time;
- 1.2.7. A reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and
- 1.2.8. All headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

1.3. Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

- 1.3.1. as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;
- 1.3.2. as between the provisions of this Agreement and the Schedules / Annexures, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules/Annexures; and
- 1.3.3. as between any value written in numerals and that in words, the value in words shall prevail.

1.4. Law Governing Contract

This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Applicable Laws of India.

1.5. Legal Jurisdiction

Any dispute arising out of this agreement shall be subject to the exclusive jurisdiction of courts in Bhubaneswar, Odisha.

1.6. Language

This Contract has been executed in English, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.

1.7. Notices

- 1.7.1. Any notice, request or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent to such Party at the address specified in the SC.
- 1.7.2. A Party may change its address for notice hereunder by giving the other Party notice in writing of such change to the address specified in the SC.
- 1.7.3. Authorized Representatives: Any action required or permitted to be taken, and any document required or permitted to be executed under this Contract by the Purchaser or the Solution Provider may be taken or executed by the officials specified in the SC.
- 1.7.4. Taxes and Duties: All taxes would be paid on actuals as per applicable laws.

1.8. Fraud and Corruption

1.8.1. Definition

It is the Purchaser's policy to require that the Purchaser as well as Solution Provider observe the highest standard of ethics during the selection and execution of the Contract. The Purchaser also requires that the Solution Provider does not demand any service charges from the Resident unless the same is agreed with the Purchaser in advance. In pursuance of this policy, the Purchaser: Defines, for the purpose of this provision, the terms set forth below as follows:

- a) "corrupt practice" means the offering, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of a public official in the selection process or in contract execution;
- b) "fraudulent practice" means a misrepresentation or omission of facts in order to influence a procurement process or the execution of a contract with the Purchaser; and includes collusive practice among bidders, prior to or after proposal submission, designed to establish bid prices at artificially high or non-competitive levels and to deprive the Purchaser of the benefits of free and open competition.
- c) "collusive practices" means a scheme or arrangement between two or more bidders, with or without the knowledge of the Purchaser, designed to establish prices at artificial, non-competitive levels;
- d) "coercive practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process, or affect the execution of a contract;
- e) "unfair trade practices" means supply of services different from what is ordered on, or change in the Scope of Work which was agreed to;

1.8.2. Measures to be taken by the Purchaser

- a) The Purchaser may terminate the contract if it is proven that at any time the representatives or employees of the Solution Provider were engaged in corrupt, fraudulent, collusive or coercive practices during the execution of the contract, without the Solution Provider having taken timely and appropriate action satisfactory to the Purchaser to remedy the situation;
- b) The Purchaser may also sanction against the Solution Provider, including declaring the Solution Provider ineligible stated period of time (as decided by purchaser), to be awarded a contract if it at any time it is proven that that the Solution Provider has, directly or through an agent, engaged in corrupt, fraudulent, collusive or coercive practices in competing for, or in executing, a Purchaser-financed contract.

2. COMMENCEMENT, COMPLETION, MODIFICATION & TERMINATION OF CONTRACT

2.1. Term of Contract

The term under this Contract will be for a period of 64 months which shall start from effective date of each work order.

2.2. Extension of Contract

- 2.2.1. If required by the Purchaser, an extension of the term can be granted to the Solution Provider. The final decision will be taken by the Purchaser.
- 2.2.2. The Purchaser shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the Solution Provider, at least one month before the expiration of the term hereof, whether it will grant the Solution Provider an extension of the term. The decision to grant or refuse the extension shall be at the Purchaser's discretion.
- 2.2.3. Where the Purchaser is of the view that no further extension of the term be granted to the Solution Provider, the Purchaser shall notify the Solution Provider of its decision at least one month prior to the expiry of the Term. Upon receipt of such notice, the Solution Provider shall continue to perform all its obligations hereunder, until such reasonable time beyond the term of the Contract with the Purchaser.

2.3. Termination of Contract

- 2.3.1. Normal termination of the contract would happen at the end of the tenure.
- 2.3.2. Pre-mature termination of the contract would happen in case of insolvency of bidder or due to conditions of breach happening due to reasons solely and entirely attributable to Bidder, provided prior thirty days written notice to rectify the same is given by the OCAC and failure by Bidder to rectify in the notice period.
- 2.3.3. Termination by Solution Provider - The Solution Provider may terminate this Contract, by not less than Ninety (90) days' written notice to the OCAC, such notice to be given after the occurrence of any of the following events –
 - a) If the Purchaser fails to pay any money due to the Solution Provider pursuant to this Contract and not subject to dispute pursuant to Clause 7.10 hereof within forty-five (45) days after receiving written notice from the SI that such payment is overdue.
 - b) If the Purchaser fails to comply with any final decision reached as a result of arbitration pursuant to Clause 7.10 hereof

- c) If the Purchaser is in material breach of its obligations pursuant to this Contract and has not remedied the same within forty-five (45) days (or such longer period as the Solution Provider may have subsequently approved in writing) following the receipt by the Purchaser of the Solution Provider's notice specifying such breach.
- d) OCAC failure to give acceptance of deliverables in mutually agreed time schedules

2.4. Effects of Termination

- 2.4.1. In the event of a pre-mature termination of this agreement by OCAC, the compensation payable to bidder will be decided in accordance with the Terms of Payment schedule for the milestones completed services and accepted deliverables till the last effective date of termination.
- 2.4.2. Parties shall mutually agree upon a transition plan and comply with such a plan. The bidder shall agree to extend full cooperation in supporting the transition process.

2.5. Binding Clause

All decisions taken by the Purchaser regarding the processing of the Contract shall be final and binding on all parties concerned.

2.6. Modifications or Variations

Any modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope of the Services, may be made by written communication between the Parties and after Prior Mutual consent by both the parties. However, each Party shall give due consideration to any proposals for modification or variation made by the other Party.

2.7. Force Majeure

- 2.7.1. Any delay in or failure of the performance shall not constitute default hereunder or give rise to any claims for damage, if any, to the extent such delays or failure of performance is caused by occurrences such as acts of god or an enemy, expropriation or confiscation of facilities by Government authorities, acts of war, rebellion, sabotage or fires, floods, explosions, terrorist activities, military operations, riots, epidemics, civil commotions, strikes etc. The Solution Provider shall keep records of the circumstances referred to above and bring these to the notice of Government of Odisha in writing immediately on such occurrences. The amount of time, if any, lost on any of these counts shall not be counted for the Contract period. The decision of the Purchaser arrived at after consultation with the Solution Provider, shall be final and binding. Such a determined period of time will be extended by the Purchaser to enable the Solution Provider to complete the job within such

extended period of time. If a Solution Provider is prevented or delayed from performing any of its obligations under the Contract with Purchaser by Force Majeure, then the Solution Provider shall notify the Purchaser the circumstances constituting the Force Majeure and the obligations of which is thereby delayed or prevented, within five (5) working days from the occurrence of the events.

- 2.7.2. In the event the Force Majeure substantially prevents, hinders or delays a Solution Provider's performance of Services for a period in excess of five (5) working days from the occurrence of any such event, the Solution Provider may declare that an emergency exists. Post the emergency is declared to be over, the Purchaser will communicate to the Solution Provider to resume normal services within a period of seven (7) days. In the event that the Solution Provider is not able to resume services within the next seven days, the Purchaser may terminate the Contract and/or obtain substitute performance from an alternate Solution Provider.
- 2.7.3. Solution Provider will advise, in the event of his having to resort to this Clause, in writing, duly certified by the statutory authorities, the beginning and end of the causes of the delay, within fifteen (15) days of the occurrence and cessation of such Force Majeure.

2.8. No Breach of Contract

The failure of a Party to full fill any of its obligations under the contract shall not be considered to be a breach of, or default under, this Contract insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.

Measures to be Taken

- 2.8.1. A Party affected by an event of Force Majeure shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall take all reasonable measures to minimize the consequences of any event of Force Majeure.
- 2.8.2. A Party affected by an event of Force Majeure shall notify the other Party of such event as soon as possible, and in any case not later than fourteen (14) days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give written notice of the restoration of normal conditions as soon as possible.
- 2.8.3. Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

- 2.8.4. During the period of their inability to perform the Services as a result of an event of Force Majeure, the Solution Provider, upon instructions by the Purchaser, shall either:
- a) Demobilize or
 - b) Continue with the Services to the extent possible, in which case the Solution Provider shall continue to be paid proportionately and on pro rata basis, under the terms of this Contract.
- 2.8.5. In the case of disagreement between the Parties as to the existence or extent of Force Majeure, the matter shall be settled according to Clause GC 8 (Settlement of dispute).

3. OBLIGATIONS OF THE SOLUTION PROVIDER

3.1. Scope of Work and Deliverables

This will be in conformity with the Scope of Work and Deliverables specified in the RFP document and shall include the submissions made by the bidder in their proposal and work plans, further refined during the negotiations. Deliverables and milestones shall be established with a process of formal acceptance or measurable criteria. In case of any conflict between RFP and Proposal submitted by the Bidder in relation to Scope of Work or Deliverables, the Proposal submitted by Bidder (including clarifications, if any) shall prevail and apply.

3.2. Norms Governing Service Delivery

- 3.2.1. Provide necessary performance guarantees on signing of the agreement;
- 3.2.2. Shall deliver the services in a professional manner commensurate with accepted industry practices and/or technical standards which are generally expected of such an engagement;
- 3.2.3. Bidders shall establish a formal team structure with a named Project Manager who will serve as single point of contact and staff with competent resources to provide effective and expert service delivery, in tune to the requirements;
- 3.2.4. Provide a roadmap and project plan for this engagement, describing clearly the responsibilities, timelines, dependencies, milestones and risks;
- 3.2.5. The cost of travel & accommodation during visit to various places of Odisha for various works like system study, training etc. should be borne by the bidder.

3.3. Standard of Performance

The Solution Provider shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The Solution Provider shall always act, in respect of any matter relating to this Contract or to the Services, as faithful advisers to the Purchaser, and shall at all times support and safeguard the Purchaser's legitimate interests in any dealings with third Parties.

3.4. Conflicts of Interest

The Solution Provider will be barred from participating in any Bid Process (downstream activities) falling within the Scope of Work / assisted by the Solution Provider or its personnel, till the duration of their Contract with the Purchaser in the department in which the Solution Provider is providing its services under this Contract. The Solution Provider would not be barred from executing existing projects for which it is already selected within the department, however it would be barred from any future projects / Bid Process (downstream activities) falling within the Scope of Work / assisted by the Solution Provider or its personnel, till the duration of their Contract with the Purchaser. The Solution Provider, if selected for any consultancy work, shall not be allowed to work in any downstream activity like application development, maintenance, support, hardware/software supply etc. in the same project. Similarly, the Solution Provider selected as the consultant shall not be allowed to work as Solution Provider and vice-versa in the same project.

3.5. General Confidentiality

Except with the prior written consent of the Purchaser or its client department/organisation, the Solution Provider and the Personnel shall not at any time communicate to any person or entity any confidential information acquired in the course of the Services, nor shall the Solution Provider and the Personnel make public the recommendations formulated in the course of, or as a result of, the Services.

3.6. Intellectual Property Rights (IPR)

The source code of entire applications (except OEM products/solutions) along with necessary documentations developed under this RFP/Contract should be shared with OCAC after Go-live of the application.

3.7. Assignment

The Solution Provider shall not assign, in whole or in part, their obligations under this Contract without the permission of Purchaser.

3.8. Force Majeure

Neither Party to this agreement shall be liable to the other for delay or default in performance of its obligations or any loss or damage which may be suffered by the other directly due to a Force Majeure event provided that the affected Party notifies the other Party of such event and its likely effects and duration as soon as possible and takes all reasonable steps to mitigate the losses/disruption.

3.9. Governing Law and Jurisdiction

This agreement and all questions of its interpretation shall be construed in accordance with the Laws of India in the High Court at Cuttack having jurisdiction. Suits, if any arising out of the contract/agreement shall be filed by either party in a court of Law to which the Jurisdiction of the High Court of Odisha extends.

3.10. Audit

- 3.10.1. The software and documents prepared for this project are subject to audit. The bidder should help OCAC during preparation of compliances of audit without any additional cost.
- 3.10.2. Software including source code, licenses (if any) and all technical documents/manuals shall be in favour of the OCAC and shall be submitted to the OCAC before final payment or on demand.
- 3.10.3. All records pertaining to this work shall be made available to the OCAC and its authorized agencies upon request for verification and/or audit, on the basis of a written request.

3.11. Good Faith

The Parties undertake to act in good faith with respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract.

3.12. Operation of the Contract

The Parties recognize that it is impractical in this Contract to provide for every contingency which may arise during the life of the Contract, and the Parties hereby agree that it is their intention that this Contract shall operate fairly as between them, and without detriment to the interest of either of them, and that, if during the term of this Contract either Party believes that this Contract is operating unfairly, the Parties will use their best efforts to agree on such action as may be necessary to remove the cause or causes of such unfairness, but no failure to agree on any action pursuant to this Clause shall give rise to a dispute subject to arbitration in accordance with Clause GC 8 hereof.

4. SETTLEMENT OF DISPUTES

- 4.1. The Purchaser and the Solution Provider shall make every effort to resolve amicably by direct informal negotiation on any disagreement or dispute arising between them under or in connection with the Contract.
- 4.2. If, after thirty (30) days from the commencement of such informal negotiations, the Purchaser and the Solution Provider have been unable to resolve amicably a Contract dispute, the dispute should be referred to the Chief Executive Officer, OCAC for resolution.
- 4.3. If, after thirty (30) days from the commencement of such reference, Chief Executive Officer, OCAC have been unable to resolve amicably a Contract dispute between the Purchaser and the Solution Provider, either party may require that the dispute be referred to the Commissioner-cum-Secretary to Govt., E&IT Department, Govt. of Odisha.
- 4.4. Any dispute or difference whatsoever arising between the parties (Purchaser and Solution Provider) to the Contract out of or relating to the construction, meaning, scope, operation or effect of the Contract or the validity of the breach thereof, which cannot be resolved through the process specified above, shall be referred to a sole Arbitrator to be appointed by mutual consent of both the parties herein. In the event the parties cannot agree to sole arbitrator, such arbitrator shall be appointed in accordance with the Indian Arbitration and Conciliation Act, 1996.
- 4.5. The arbitration proceedings shall be held at Odisha and the language of the arbitration shall be English

5. ADHERENCE TO SAFETY PROCEDURES, RULES & REGULATIONS

- 5.1. The Solution Provider shall take all measures to ensure compliance with all applicable laws and shall ensure that the Personnel are aware of consequences of non-compliance or violation of laws including Information Technology Act, 2000 (and amendments thereof).
- 5.2. Statutory Audit
 - a) The deliverables prepared for this project are subject to audit (by CAG or other entities). The bidder should help OCAC during preparation of compliances of audit without any additional cost.
 - b) All technical documents/deliverables shall be in favour of the OCAC and shall be submitted to the OCAC before final payment or on demand.
 - c) All records pertaining to this work shall be made available to the OCAC and its authorized agencies upon request for verification and/or audit, on the basis of a written request.

6. LIMITATION OF LIABILITY

Except in cases of gross negligence or wilful misconduct: -

- 6.1. neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier/ selected bidder to pay liquidated damages to the Purchaser; and
- 6.2. Maximum liability of the bidder for this project will be limited to the total value of the contract or the amount actually paid to the bidder whichever is lower and will not include any indirect or consequential clause or damage, loss or profit, data or revenue.

7. INDEMNITY

- 7.1. The Solution Provider shall indemnify the Purchaser from and against any costs, loss, damages, expense, claims including those from third parties or liabilities of any kind howsoever suffered, arising or incurred inter alia during and after the Contract period out of:
 - a) Any negligence or wrongful act or omission by the Solution Provider or any third party associated with Solution Provider in connection with or incidental to this Contract or;
 - b) Any breach of any of the terms of this Contract by the Solution Provider, the Solution Provider's Team or any third party
 - c) Any infringement of patent, trademark/copyright arising from the use of the supplied goods and related services or any party thereof
- 7.2. The Solution Provider shall also indemnify the Purchaser against any privilege, claim or assertion made by a third party with respect to right or interest in, service provided as mentioned in any Intellectual Property Rights and licenses
- 7.3. All indemnification obligations shall be subject to the Limitation of Liability clause.

8. ACTION AND COMPENSATION IN CASE OF DEFAULT

- 8.1. Conditions for default:
 - a) The deliverables at any stage of the project as developed/ implemented by the Solution Provider do not take care of all or part thereof of the Scope of Work as agreed and defined under the Contract with the Purchaser.
 - b) The deliverables at any stage of the project as developed/ implemented by the Solution Provider fails to achieve the desired result or do not meet the intended quality and objective as required by the Purchaser.
 - c) The documentation is not complete and exhaustive.
 - d) There is a change in resource before the completion of a pre-defined period.

- 8.2. The Purchaser may impose penalties on the Solution Provider providing the Services as per the Service Levels defined under this Contract.

9. SERVICE LEVEL AND PENALTY

As per RFP

10. PAYMENT TERM

- 10.1. The total fees payable to the bidder including a milestone based payment in the RFP would be specified. Such payments shall be inclusive of all taxes / levies and other out of pocket expenses. Rate of taxes will be applicable as per the rate prevailing at the time of submission of Bill.
- 10.2. Payments for additional services in case of change in scope will also be specified.
- 10.3. In case of a bona fide dispute regarding any invoice, OCAC shall be entitled to delay or withhold payment of the invoice or part of it, limited to the extent of the disputed amount.

11. MISCELLANEOUS PROVISIONS

- 11.1. Any failure or delay on part of any Party to exercise right or power under this Contract shall not operate as waiver thereof.
- 11.2. The Solution Provider shall notify the Purchaser of any material change in their status, in particular, where such change would impact performance of obligations under this Contract.
- 11.3. The Solution Provider shall at all times indemnify and keep indemnified the Purchaser against all claims/damages for any infringement of any copyrights while providing its services under the Project.
- 11.4. The Solution Provider shall at all times indemnify and keep indemnified the Purchaser against any claims in respect of any damages or compensation payable in consequences of any accident or injury sustained or suffered by its employees or agents or by any other third Party resulting from or by any wilful action or gross negligence by or on behalf of the Solution Provider.
- 11.5. The Solution Provider shall at all times indemnify and keep indemnified the Purchaser against any and all claims by Employees, agent(s), employed engaged or otherwise working for the Solution Provider, in respect of wages, salaries, remuneration, compensation or the like.
- 11.6. All claims regarding indemnity shall survive the termination or expiry of the Contract.

- 11.7. All materials provided to the Purchaser by Solution Provider are subject public disclosure laws such as RTI etc. except in respect of exclusions set out in such laws.
- 11.8. The Solution Provider shall not make or permit to be made a public announcement or media release about any aspect of the Contract without a written consent from the Purchaser
- 11.9. The Solution Provider shall not assign/outsources/sub-contract the project to any other agency, in whole or in part, to perform its obligation under this agreement.

12. SPECIAL CONDITIONS OF CONTRACT

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

12.1. The addresses are

For the Purchaser	For the Solution Provider
Odisha Computer Application Centre (OCAC) Designated Technical Directorate of Electronics & Information Technology Department, Government of Odisha, Plot No.: N-1/7-D, PO: RRL, Acharya Vihar Square, Bhubaneswar-751013, Odisha, India, Tel: 0674 - 2567064 / 2567858/ 2586838, Email: gm_ocac@ocac.in	

12.2. The Authorized Representatives are

For the Purchaser	For the Solution Provider
General Manager (Admn.) Odisha Computer Application Centre (OCAC) Designated Technical Directorate of Electronics & Information Technology Department, Government of Odisha, Plot-N- 1/7-D, Po-RRL, Acharya Vihar Square, Bhubaneswar - 751013, Odisha, India	

12.3. Contract Schedule

The Solution Provider	M/s
The effective date of the Contract/Work Order	
The date for the commencement of services	

Contract period	5 years 4 months from the effective date of contract/work order
-----------------	---

12.4. Cost of Services

The cost of service as per Commercial Bid of the successful bidder is described at **Appendix-C – Cost of Services**

12.5. Bank Account Details

All payment under this contract shall be made by Electronic Transfer to the account of the Solution Provider with (Bank & Account No.):

Bank	
Branch	
IFS Code	
Account Number	

Payment will be made by the purchaser to the Solution Provider /Departments as per the contract value agreed in the contract as follows:

12.6. APPLICABILITY OF TENDER TERMS AND CONDITIONS

All terms & conditions stated in this Agreement would override the terms & conditions mentioned in the RFP (No: OCAC-SEGP-SPD-0010-2021-21012) and Technical & Commercial bid submitted by bidder. However, all other terms & conditions except those mentioned in this agreement would be applicable as per RFP.

Binding signature of Purchaser Binding signature of Solution Provider

Signed By: _____

Signed

By:

In the presence of (Witnesses)

(1).....(1).....
(2)..... (2).....

As per RFP

Resource Deployment Plan submitted by Bidder as per the requirement specified in the RFP.

As per the Commercial Bid of the successful bidder