Request for Proposal (RFP)

for

Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC)

Tender document no:OCAC-TE-17/2018(P-I)/ENQ-20030

Odisha Computer Application Centre (OCAC)

(Technical Directorate of E&IT Department, Govt. of Odisha)
OCAC Building, Plot No.-N-1/7D, Acharya Vihar, RRL Post Office,
Tel No: - 0674-2567280/2567064/2567295/2588283

Table of Contents

----------This page has been intentionally kept blank----------

Disclaimer

The information contained in this Tender document or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by Odisha Computer Application Centre (OCAC) or any of their employees is provided to Bidder(s) on the terms and conditions set out in this Tender Document and such other terms and conditions subject to which such information is provided. This Tender is not an agreement and is neither an offer nor invitation by the OCAC to the Bidders or any other person. The purpose of this Tender is to provide interested parties with information that may be useful to them in making their technical and financial offers pursuant to this Tender (the "Bid"). This Tender includes statements, which reflect various assumptions and assessments arrived at by the OCAC in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This Tender may not be appropriate for all persons, and it is not possible for the OCAC, to consider the technical capabilities, investment objectives, financial situation and particular needs of each party who reads or uses this Tender. The assumptions, assessments, statements and information contained in this Tender, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigations, studies and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this Tender and obtain independent advice from appropriate sources. Information provided in this Tender to the Bidder(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. OCAC accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein. OCAC, makes no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this Tender or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the Tender and any assessment, assumption, statement or information contained therein or deemed to form part of this Tender or arising in any way in this Bid Stage. OCAC also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this Tender. OCAC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this Tender. The issue of this Tender does not imply that OCAC is bound to select a Bidder or to appoint the Preferred Bidder, as the case may be, for the Project and OCAC reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever. OCAC reserves all the rights to cancel, terminate, change or modify this selection process and/or requirements of bidding stated in the Tender, at any time without assigning any reason or providing any notice and without accepting any liability for the same. The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by OCAC or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and OCAC shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process.

1. Introduction

Odisha Computer Application Centre (OCAC), the Designated 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. So it helps IT to reach the common citizen so as to narrow down the Digital Divide and widespread applications of IT is establishing a system where the citizens are receiving good governance ensuring speed of decisions from a transparent Government through an effective e-Governance System.

Computer Emergency Response Team – Odisha (CERT-O)

In the wake of lack of adequate expertise in Government/Government Agencies/ there emerged a need for setting up of a permanent mechanism which would act as nodal agency for monitoring various cyber security related matters for Government of Odisha/Government Organisations. The state government had therefore felt the necessity for setting up of Computer Emergency Response Team-Odisha (CERT-Odisha or CERT-O) in line with CERT India (CERT-IN) to cater to crisis situations in Cyber Security matters of Government of Odisha.

Cyber Security Operation Centre (CSOC)

A cyber security operations centre or CSOC is a subgroup of CERT-O and comprises of a team of expert individuals and the facility in which they dedicate themselves entirely to high-quality IT security operations. A CSOC seeks to prevent cybersecurity threats and detects and responds to any incident on the computers, servers and networks it oversees. What makes a CSOC unique is the ability to monitor all systems on an ongoing basis, as employees work in shifts, rotating and logging activity around the clock.

In recent times organizations are shifting their focus more on the human element than the technology element to assess and mitigate threats directly rather than rely on a script. While technology systems such as Firewall, IPS or other security appliances may prevent basic attacks, human analysis is required to put major incidents to rest.

As opposed to a traditional IT department, a CSOC staff primarily includes a team of highly experienced cybersecurity analysts and trained professionals. These individuals use a range of computer programs and specialized security processes that can pinpoint weaknesses in the department's infrastructure and prevent these vulnerabilities from leading to intrusion or theft.

Ensuring these programs comply with company, industry and government regulations is also a significant part of a CSOC's job.

With a variety of tasks to perform, using a variety of tech and methods, SOCs can look different depending on a multitude of factors. Some companies, Govt. Departments, PSU sectors have an in-house CSOC, while others opt to outsource these services. Most importantly, however, they all have the primary goal of preventing breaches and minimizing losses due to online criminal activity.

Objective

Government of Odisha (GoO), Electronics & Information Technology Department and Odisha Computer Application Centre (OCAC) intends to take high priority in securing the organization's and departmental data and removal of any threat that exist in the current infrastructure of the organization / department. Additionally, its objective is to ensure minimum dwell time of any possible threat in servers, networks and systems. This is possible only if there is a system in place that has constant monitoring. Establishing a Cyber Security Operations Centre (CSOC) has become more important for organizations as security breaches are on the rise and the cost associated with data loss is often high.

Hence developed the vision of establishing a Cyber Security Operations Centre to precisely tackle this problem and be better prepared for a worst-case scenario. At present there is no integrated system in place to monitor the infrastructure, network flow, data flow and intrusion for the organization(s). The monitoring currently is done at individual department or project (SDC / SWAN) level and is not integrated into a centralized information and monitoring system. The technology utilized by the individual department / project does not cater to all the infrastructure and are equipped with limited resources.

In brief the objectives can be distinguished as below:-

- Prevention of cyber security incidents through various measures as establishing security policy, continuous threat analysis, deployment of preventive and detective security devices.
- Monitoring, detection and analysis of potential intrusions/threats in real time from security related data sources.
- Response to the threats in timely manner for mitigate.
- Capacity building and awareness creation for cyber security.

Cyber security operations centre (CSOC) would be a command centre facility for a team of IT professionals with expertise in information security that would be responsible for monitoring, analysing and protecting the organization from cyberattacks. In the CSOC, internet traffic, local area network, desktops, servers, databases, applications and other systems would be continuously examined for signs of a security incident. The CSOC staff may work with other teams or departments, but would typically be self-contained with employees that have high-level information technology and cybersecurity skills.

2. Acronyms

List of acronym that has been used in this document has mentioned here along with its full form/meaning.

Sr. No.	Abbreviations	Description/ Definitions
1.	AC	Air Conditioning
2.	AHU	Air Handling Unit
3.	APT	Advanced Persistent Threats
4.	BOM	Bill of Material
5.	BOQ	Bill of Quantity
6.	BTA	Business Transaction Activity
7.	CAPEX	Capital Expenditure
8.	CCTV	Closed Circuit Television
9.	CSOC	Cyber Security Operations Centre
10.	Cu	Copper
11.	DB	Distribution Box
12.	DC	Data Centre
13.	DPR	Detailed Project Report
14.	DOT	Department of Telecom
15.	EPS	Events per second
16.	FAT	Final Acceptance Test
17.	FTP	File Transfer Protocol
18.	G2B	Government to Business
19.	G2C	Government to Citizens
20.	G2G	Government to Government
21.	GI	Galvanized Iron
22.	GoO	Government Of Odisha
23.	IA	Implementation Agency
24.	IGBT	Insulated Gate Bipolar Transistor
25.	IP	Internet Protocol
26.	IPS	Intrusion Prevention System
27.	IOT	Internet over Things
28.	ISMC	Indian Standard Medium Channel
29.	ISO	International Organization for Standardization
30.	ISP	Internet Service Provider
31.	IT	Information Technology
32.	KV	Kilo Volt

Sr. No.	Abbreviations	Description/ Definitions
33.	LAN	Local Area Network
34.	LoI	Letter of Intent
35.	MCB	Miniature Circuit Breaker
36.	MCCB	Moulded Case Circuit Breaker
37.	MeitY	Ministry of Electronics and Information Technology
38.	NOC	Network Operations Centre
39.	NVR	Network Video Recorder
40.	O&M	Operations and Maintenance
41.	OCAC	Odisha Computer Application Centre
42.	OEM	Original Equipment Manufacturer
43.	OPEX	Operational Expenditure
44.	OSDC	Odisha State Data Centre
45.	PAT	Partial Acceptance Test
46.	PDU	Power Distribution Unit
47.	PMU	Project Management Unit
48.	PoE	Power over Ethernet
49.	PVC	Poly Vinyl Chloride
50.	QOS	Quality of Services
51.	RFP	Request For Proposal
52.	SAN	Storage Area Network
53.	SDC	State Data Centre
54.	SIEM	Security Information and Event Management
55.	SOAR	Security Orchestration Automation and Response
56.	SOP	Standard Operating Procedure
57.	STP	Spanning Tree Protocol
58.	SWAN	State Wide Area Network
59.	TCP	Transmission Control Protocol
60.	UAT	User Acceptance Test
61.	UPS	Uninterrupted Power Supply
62.	WAN	Wide Area Network

3. Invitation for bid

Odisha Computer Application Centre invites offer / proposal from interested bidders for "Design, Build, Installation, Commissioning, Operation & Maintenance of Non-IT & IT infrastructure for Cyber Security Operations Centre, Odisha" for a period of four (4) years from date of Go-live of CSOC. This RFP document is being published on web portal "https://www.ocac.in", this section provides general information about the issuer, important dates, and addresses for bid submission & correspondence for the bidders.

The bidders are advised to study the RFP document carefully. Submission of bids shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

About OCAC

Odisha Computer Application Centre is the nodal agency of Odisha State working towards 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 generate 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.

3.1 Bid Schedule

The Bid document may be purchase by any interested Bidder on submission of a written application along with the Bid document fee of Rs. 25,000 /- in the form of Demand Draft from a scheduled bank in India in favour of Odisha Computer Application Centre, payable at Bhubaneswar, during office hours on any working day. The complete bid document has also been published on the website www.ocac.in or www.odisha.gov.in for downloading. The downloaded bid document shall also be considered valid for participation in the bid process but such bid documents should be submitted along with the required Bid document fee as mentioned.

Proposal inviting agency	**Odisha Computer Application Centre, Bhubaneswar.**
Non Refundable RFP Cost	Rs. 25,000/- (Twenty Five Thousand only) plus GST 12% DD / Bankers Cheque in favour of "OCAC" payable at Bhubaneswar from a nationalized / scheduled commercial bank in India.
Sale of RFP Document	**From date: 24-09-2020 to 27-10-2020, 2:00 P.M.** Also download from our website www.ocac.in
The contact information	General Manager (Admin) Odisha Computer Application Centre, N1/ 7D, Acharya Vihar Square, Near Planetarium, P.O. – RRL, Bhubaneswar 751013 Ph. - 0674-2582850/ 2588064 Website: www.ocac.in

Last date and time for submission of proposal	**Date:27-10-2020 Time:03:00 P.M.**
Earnest Money Deposit - (EMD)	Rs. 50,00,000/- (Fifty lakhs only) in form of Bank Guarantee in the prescribed format in favour of "OCAC" payable at Bhubaneswar from a nationalized / scheduled commercial bank in India.
Pre bid Conference and clarifications	On 30-09-2020 (Bidder pre-bid queries should reach as on before **date:30-09-2020 time:04:00 P.M.**) Bidders should email their pre-bid queries to: **"saroj.tripathy@ocac.in" or "gm_ocac@ocac.in"** with subject line "**Odisha CSOC: Pre-bid queries against RFP Enq. no. 20030**"
Opening of General cum Technical Presentation by the qualified bidder.	**27-10-2020, 04:00 P.M.**
Opening of Commercial Bids	Will be intimated later
Address for Correspondence and bid submission	General Manager (Admin), OCAC, Odisha Computer Application Centre, N1/ 7D, Acharya Vihar Square, Near Planetarium, P.O. – RRL, Bhubaneswar 751013 Ph. - 0674-2582850/ 2588064 Website: www.ocac.in
Language of the proposal	This proposal should be filled in English language only. If any supporting documents are to be submitted, in any other language other than English, then translation of the same in English language, attested by the Bidder should be attached.
Proposal currency	Prices shall be quoted in Indian Rupees (INR)

3.2 Validity of bid document

Bids shall remain valid for a period of 180 days after the last date of submission of proposal as mentioned in Section 3.1 or as may be extended from time to time. OCAC holds the right to reject a bid valid for a period shorter than 180 days as non-responsive, without any correspondence. In exceptional circumstances, prior to expiry of the bid validity period, OCAC may request the bidders' consent to an extension of the validity period. The request and response shall be made in writing. Extension of validity period by the bidder should be unconditional and irrevocable. The EMD / Bank Guarantee provided shall also be suitably extended. A bidder may refuse the request without forfeiting the bid security.

3.3 Due Diligence

The Bid shall be deemed to have been submitted after careful study and examination of this RFP document. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information or submission of a bid not responsive to this RFP will be at the Bidders" risk and may result in rejection of the bid. Also the grounds for rejection of Bid should not be questioned after the final declaration of the successful Bidder.
The Bidder is requested to carefully examine the RFP documents and the terms and conditions specified therein, and if there appears to be any ambiguity, contradictions, inconsistency, gap and/or discrepancy in the RFP document, bidder should seek necessary clarifications by e-mail as mentioned in Section 3 of the RFP.

Failure to comply with the requirements of this paragraph may render the Proposal non-compliant and the Proposal will be rejected. Bidders must:

a. Comply with all requirements as set out within this RFP.
b. Submit the forms as specified in this RFP and respond to each element in the order as set out in this RFP.
c. Include all supporting documentations specified in this RFP.

3.4 Pre-bid conference

- OCAC shall hold a pre-bid conference with the prospective bidders on **03-10-2020 at 4:00 P.M.**
- The Bidders will have to ensure that their queries for Pre-Bid conference should be sent to the e-mail id: saroj.tripathy@ocac.in on or before date **30-09-2020 by 4:00 P.M.**
- Queries submitted after the scheduled date and time, shall not be accepted.
- The queries should necessarily be submitted in the following format:

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Reference / Subject Clarification
1.				
2.				

3.5 General Instructions to bidders

- One bidder is eligible to submit only one bid proposal. If any bidder is found to be submitting more than one proposal, any one proposal would be considered and rest of the proposal submitted by the bidder would be disqualified.

- While every effort has been made to provide comprehensive and accurate background information, requirements, and specifications, Bidders must form their own conclusions about the requirements or contact OCAC for any clarification. Bidders and recipients of this RFP may wish to consult their own legal advisers in relation to this RFP.

- All necessary tools and accessories required to complete the scope of work as per RFP document is in the scope of the bidder, at no extra cost to OCAC.

- All information to be supplied by Bidders will be treated as contractually binding on the Bidders, on successful award of the assignment by OCAC on the basis of this RFP.

- The bidder should put signature and seal of the authorized personnel on each and every page of the bid document.

- The certifications of the manpower resources proposed for the project should be valid during the bid submission and also for the entire duration of the project. Bidder should ensure to reissue any expired certification from the relevant body.

- 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 with 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.

- This RFP supersedes and replaces any previous public documentation & communications in this regard and bidders should place no reliance on such communications.

- OCAC at any time during the evaluation period may contact the personnel authorized by the bidder for clarification of information / documentation submitted by the bidder.

- The bidder may propose "Make in India" products and solutions in their bid, however the products / solutions should be in compliance with the required guidelines and standards. They should also meet the criteria and minimum requirement as mentioned in the RFP document.

- The bidder shall be responsible for the upgradation and additional configuration of the SIEM (ArcSight ESM) solution, Logger appliances, Connector appliances and User Behavioural Analyser (UBA) appliance which are installed at Odisha State Data Centre.

- In case the bidder does not intend to utilize or leverage the existing SIEM / ESM solution and logger appliances deployed at Odisha State Data Centre, the bidder may be given an option to propose a new SIEM / ESM solution along with required logger and connector devices. The proposed solution may be added as per the Proforma 20 of the RFP document. However, the bidder would be responsible for the integration of the existing solutions with SOC.

- Any solution if required to be in the form of either appliance or software altogether with its requirement is to be proposed by the bidder.

- Consortium or subcontracting of any kind shall not be acceptable for this project. Any deviation would lead to disqualification or termination of the same. However, as per the State ICT Policy 2014 clause 5.5.2, it is mandated that the successful bidder must associate a local enterprise, who has not been debarred / black listed by state Government. The involvement / association of the local enterprise is limited to maximum 25% of the total project. The work allotted to the local enterprise may be limited to any one of the following:
  i. Civil and interior works of the SOC sites.
  ii. Installation, maintenance and support of the Non-IT items for SOC.
  iii. Manpower deployed for SOC.

  The local enterprise should have relevant experience, expertise and reach in the associated scope of work or activity. The successful bidder has to submit scope of work, credential and experience details of the local enterprise with OCAC.

3.6 Right to Terminate the Process

- 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.

- This RFP does not constitute as an offer by OCAC. The bidder's participation in this process may result OCAC selecting the bidder to engage towards execution of the agreement.

3.7 Confidential Information

OCAC and successful bidder shall keep every information related to the work order / engagement, project status, data and reports confidential and without the written consent of the other party hereto, divulge to any third party any documents, data, or other information furnished directly or indirectly by the other party hereto in connection with the engagement, whether such information has been furnished prior to, during or following completion or termination of the contract.

3.8 Submission of bid

- The proposal shall be submitted in hard copy in three parts in, Part-I "RFP fees DD and EMD BG", Part-II "Eligibility cum Technical bid" and Part-III "Commercial Bid".
- The complete bid should be submitted in a single sealed envelope with complete name and address of the bidder addressed to OCAC. Inside the single envelope, all the three parts of bid (Part-I, II and III) should be in separate properly labelled sealed envelopes.

- "Eligibility cum Technical bid" would consist of two parts; "Pre-qualification compliance" & "Technical Proposal". Technical Bid proposal and Commercial Bid (consisting of the commercial proposal) shall be submitted as per format mentioned in Annexure II of the RFP document. The bidders must submit their responses as per the respective formats given in this RFP, which must be properly flagged to distinguish the required enclosures.
- The submission of bids should be as per the timelines provided in the RFP. Any deviation from the timelines would result in the disqualification of the bid.
- All information required as per the RFP should be furnished by the bidder in the specified formats provided. Any information not found or information in a different format may lead in the disqualification of the bid.
- The proposal should be signed by an authorized signatory (having power of attorney/authorized by board resolution) on each page of the proposal document including enclosures.
- The proposal shall contain no interlineations, erasures or overwriting, in order to correct error made by the Bidder. All corrections shall be done & initialled by the authorized signatory after striking out the original words / figures completely.
- Please note that prices should not be indicated in the Technical Proposal but should only be indicated in the Commercial Proposal. Any proposal with commercial notes / values / price submitted along with Technical Proposal will be summarily rejected.
- The proposal shall be submitted in hardcopy, along with RFP fee and EMD at the specified address as mentioned above within the above date and time. The validity of the EMD should have a validity of 180 days.
- Technical presentation should be made by the bidder on a date specified by OCAC, a softcopy of the presentation should also be shared by the bidder with OCAC. The technical presentation should at least contain the following contents:
    - Experiences in similar line of services for Cyber SOC.
    - Virtual walkthrough of existing Cyber SOC command centres implemented by the bidder.
    - Approach and Methodology for the implementation and O&M of Cyber SOC.
    - Provisions for upgradation and technology improvement of SOC infrastructure.
    - Resources proposed for deployment at SOC.
    - Brief demonstration of the line of services of the bidder and client base.
    - Any other value addition to the services of proposed SOC.
- Technical interview will be taken for the manpower proposed by the bidder for the operations and maintenance of the project. The interview would be limited to the SOC analysts, SOC Engineer, Security administration and Threat Intelligence expert and SOC manager. The date and time of the interview will be intimated by OCAC to the bidder.
- OCAC may, at its discretion, extend the deadline of the bid process for any administrative or any other reason.

3.9 Evaluation procedure

1. OCAC may constitute an Evaluation Committee to evaluate the responses of the bidders.
2. The Evaluation Committee constituted by OCAC shall evaluate the responses to the RFP and all supporting documents / documentary evidence. Inability to submit requisite supporting documents / documentary evidence, may lead to rejection.

3. The interpretation of the bids and the decision made by the Evaluation Committee in the evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of evaluation with the committee.
4. The Evaluation Committee may ask for meetings with the bidders to seek clarifications on their bids.
5. The Evaluation Committee reserves the right to reject any or all bids on the basis of any deviations.
6. Each of the responses shall be evaluated as per the criterions and requirements specified in this RFP.
7. Initial Proposal scrutiny will be held and incomplete details as given below will be treated as non-responsive. If Bids;
    a. Are submitted without tender fee or EMD in prescribed format.
    b. Are not submitted as specified in the RFP document.
    c. Received without the Letter of Authorization (Power of Attorney).
    d. Are found with suppression of details.
    e. With incomplete information, subjective, conditional offers and partial offers submitted.
    f. Submitted without the documents requested in the Proforma.
    g. Have non-compliance of any of the clauses stipulated in the RFP.
    h. With lesser validity period.

8. Evaluation Committee will prepare a list of responsive bidders, who comply with all the Terms and Conditions of the RFP. All eligible bids will be considered for further evaluation by a Committee according to the Evaluation process define in this RFP document. The decision of the Committee will be final in this regard. All responsive Bids will be considered for further processing as below:
    a. Evaluation committee will examine the bids to determine whether they are complete, whether any computational errors have been made, and whether the bids are generally in order. The interpretations made by the evaluation committee will be final and binding on the bidders.
    b. Reasonableness of Prices: Prices quoted by bidders must be reasonable with prevalent market rates. AHR (Abnormally High Rates) and ALR (Abnormally Low rates) shall not be accepted and OCAC shall have to the right to reject the bid.
    c. In case an item has been left out in the BOQ/BOM/Price bid by a particular bidder but required for the successful implementation of project and/or it is mentioned in the solution document of the bidder, OCAC will have the right to reject the bid or ask the bidder to supply the item free of cost.
    d. It is mandatory for bidder to submit detailed BOM (Bill of material with quantity) as unpriced bid in technical bid. Any discrepancy in price and unpriced bid will lead to disqualification of the bid OR OCAC will have the right to consider the highest amongst the BOQ/BOM and the price bid.
    e. In case of no price quoted or zero price quoted against an item by a bidder, the bidder has to provide / implement the item at zero cost.
    f. In case of a situation where the bidder has quoted abnormally low quantity or abnormally high quantity for an item, OCAC will have the rights to ask for an explanation during technical evaluation stage. The bidder will be given chance to increase or decrease the quantity as per the solution the bidder would propose and accepted by OCAC. This will not be applicable for the quantity mentioned against items that is

already asked in the tender. Accordingly during commercial evaluation the prices will be calculated for revised quantity submitted by bidder.

g. 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 an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected.
- If the Bidder does not accept the correction of the errors, his proposal will be rejected.
- If there is a discrepancy between words and figures, the amount in words will prevail.

h. OCAC may conduct clarification meetings with each or any Bidder to discuss any matters, technical or otherwise. Result of such meeting/ clarification may be published on specified website; however, no material changes in the bid shall be permitted.

i. Further, the scope of the evaluation committee also covers taking any decision with regards to the RFP Document, execution/ implementation of the project including management period.

j. Proposal shall be opened in the presence of bidders representatives who intend to attend at their cost. The bidders' representatives who are present shall sign a register giving evidence of their attendance.

Proposal document shall be evaluated as per the following steps.

- Preliminary Examination of Eligibility Criteria documents: The Eligibility document will be examined to determine whether the bidder meets the eligibility criteria, whether the proposal is complete in all respects, whether the documents have been properly signed and whether the bids are generally in order. Any bids found to be non-responsive for any reason or not meeting the minimum levels of the performance or eligibility criteria specified in various sections of this RFP Document will be rejected and will not be considered further.
- Technical Evaluation: A detailed evaluation of the bids shall be carried out in order to determine whether the bidders are competent enough and whether the technical aspects are substantially responsive to the requirements set forth in the RFP document. Bids received would be assigned scores based on the parameters defined. The technical specification and capacity of the solutions provided by the bidder would also be noted for the evaluation.
- The technically qualified bidders shall be invited during opening of the commercial bids and subsequently commercial evaluation shall be carried out.

3.10 Criteria for bidding eligibility and evaluation

3.10.1 Eligibility criteria

Only those bidders, who satisfy all the eligibility criteria as mentioned herein below, may respond. Document in support of all eligibility criteria are required to be submitted along with the Technical Bid. Offers received from the bidders who do not fulfil any of the following eligibility criteria are liable to be rejected.

Sr. No.	Pre-qualification criteria	Document to be submitted
1	A bidder with solutions developed in an entity incorporated in a country sharing a land boundary with India cannot participate in this bid.	Declaration by the bidder / OEM on their letter head that the bidder has proposed no such solutions in response to the RFP.
2	The bidder should be an established Company registered under the – Indian Companies Act, 1956/2013, or partnership firm register under LLP Act, 2008 since last 5 years as on 31st March 2019.	• Certificate of incorporation. • Certificate consequent to change of name if applicable.
3	The bidder should have a registered number of: • GST Registration. • Income Tax / PAN.	• Certificate of GST registration. • Copy of PAN / Income tax number.
4	The bidder may be either an OEM / an authorized partner of the OEM whose product bidder is proposing. (The solution proposed can be from a single or various OEMs).	In case of an OEM authorized partner, a letter of authorization (MAF) from original manufacturer for each solution / equipment must be furnished in original duly signed. Undertaking from the OEM mentioning a clause that OEM will provide support services during the complete period of the contract if the bidder authorized by them fails to perform.
5	The bidder should have a minimum average annual turnover of at least Rs. 200 Crores in the last three financial years (i.e. 2016-17, 2017-18 & 2018-19).	Audited Balance Sheets for last 3 years, i.e., 2016-17, 2017-18 & 2018-19 where financial turnover is segregated. Every sheet should be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 3 financial years. **or** A letter under the head of the chartered accountant / or firm certifying the financial turnover of the company is to be submitted with the bid.

Sr. No.	Pre-qualification criteria	Document to be submitted
6	The bidder should have positive net worth during the last three financial years (i.e. 2016-17, 2017-18 & 2018-19).	Audited Balance Sheets for last 3 years, i.e., 2016-17, 2017-18 & 2018-19 where profit or loss from similar works is segregated. Every sheet should be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 3 financial years. **or** A letter under the head of the chartered accountant / or firm certifying the profit and loss of the company from similar line of service is to be submitted with the bid.
7	The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.12.2019. SOC solution could be On-premises SOC, Managed SOC, Hybrid SOC. At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5 crore.	Relevant MSA copy / Work order copy / client satisfactory letter regarding successful implementation or ongoing of security operation centre (SOC) solution in the name of the bidder is to be submitted. The PO / letter should be in the name of the bidder and clearly mention the scope of work.
8	The bidder should have local office in Odisha or should submit a declaration for establishing an office in Odisha within one month of issuing of Letter of Intent (LoI) from OCAC.	Self-certification with office location addresses to be submitted / declaration for establishment of an office in case LoI has been awarded. The document should be on the bidder's letter head signed by the authorized signatory.
9	The bidder should not have been blacklisted by Government of India / Government of Odisha during the last three years.	An undertaking to this effect in the company's letter head signed by authorized signatory to be submitted as per Proforma 21 of the RFP document.
10	The bidder should have minimum manpower strength as per the different skill levels defined in the document: Level 1 analyst – minimum 20. Level 2 analyst – minimum 20. SME level - minimum 3. (The manpower criteria as mentioned in the Section 8.2 and 8.3 of the RFP document) All manpower should be on the pay role of the company / bidder.	An undertaking in the company's letter head signed by authorized signatory to be submitted.

Sr. No.	Pre-qualification criteria	Document to be submitted
11	The bidder should be: • ISO 9001:2008 or later certified • ISO 20000: 2018 certified • ISO 27001: 2013 certified	Copy of certificate to be submitted.

3.10.2 Technical evaluation

Sr. No.	Technical evaluation criteria	Document to be submitted	Marks distribution	
Company Profile				
1	The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.12.2019. SOC solution could be On-premises SOC, Managed SOC, Hybrid SOC. At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5 crore.	Relevant MSA copy / Work order copy / client satisfactory letter regarding successful implementation or ongoing of security operation centre (SOC) solution in the name of the bidder is to be submitted. The WO / letter should be in the name of the bidder and clearly mention the scope of work.	More than or equal to 8 Govt. / BFSI clients.	10 marks
			More than or equal to 5 and less than 8 govt. / BFSI clients.	07 marks
			More than or equal to 3 and less than 5 govt. / BFSI clients.	05 marks
2	Experience in implementation of on-premises Cyber Security operations centre.	Relevant MSA copy / Work order copy / client satisfactory letter regarding successful implementation or ongoing of security operation centre (SOC) solution in the name of the bidder is to be submitted. The WO / letter should be in the name of the bidder and clearly mention the scope of work.	More than or equal to 05 on premises CSOC projects implemented successfully / ongoing.	10 marks
			At least 03 on premises CSOC projects implemented successfully / ongoing.	07 marks
			At least 02 on-premises CSOC projects implemented successfully / ongoing.	05 marks

Sr. No.	Technical evaluation criteria	Document to be submitted	Marks distribution	
3	The proposed bidder / OEM has experience in implementing at least one project handling 20000 EPS or more	Relevant MSA copy / Work order copy / client satisfactory letter mentioning the number of EPS and the solution. The WO / letter should be in the name of the bidder / OEM and clearly mention the scope of work.	More than 50000 EPS	10 marks
			More than 30000 EPS up to 50000 EPS	07 marks
			20000 EPS up to 30000 EPS	05 marks
4	Major solutions like SOAR and SIEM should be from OEMs who have both local and global presence, deployed solutions and supported customers globally.	Declaration from the OEM mentioning the credential details and deployment of solution for customers both within and outside India.	Yes, have both national and global presence	05 marks
			No, does not have both national and global presence	00 marks
Manpower				
5	Certified CISA, CEH, CISSP, CISM, CRISC, or equivalent (any one) personnel under the payroll of the company	An undertaking in the company's letter head signed by authorized signatory to be submitted. The undertaking should mention the name and employee code of the personnel along with certification.	At least 04 CISSP, 05 CISA / CISM, 10 CEH and 06 proposed SIEM solution certified personnel and 10 personnel any one certification mentioned. Total 35 personnel.	10 marks
			At least 02 CISSP, 03 CISA /CISM, 05 CEH and 05 proposed SIEM solution certified personnel and 10 personnel any one certification mentioned. Total 25 personnel.	07 marks
			At least 03 CEH and 02 proposed SIEM solution certified personnel and 10 personnel any one certification mentioned. Total 15 personnel.	05 marks
6	Quality of the CVs of resources proposed for the CSOC project	The quality / scoring of CVs would be	CV of resource proposed for SOC Manager	Maximum 02 mark

Sr. No.	Technical evaluation criteria	Document to be submitted	Marks distribution	
		considered on basis of years of relevant experience, qualification, certification, projects associated with, etc. The process would be held under a technical panel of OCAC.	CV of resource proposed for Security administration and Threat Intelligence expert	Maximum 02 mark
			CV of resources proposed for CSOC Engineer - 0.5 marks for each resource	Maximum 1.5 marks
			CV of resources proposed for Level 2 analyst - 0.5 marks for each resource	Maximum 3.5 marks
			CV of resources proposed for Level 1 analyst - 0.5 marks for each resource	Maximum 3.5 marks
7	Quality of resources to be proposed for CSOC operations	The quality / scoring of resources would be considered through interviews to be held through a technical panel of OCAC. The interview for CSOC Engineer, Level 1 analyst and Level 2 analyst will be held collectively and not on individual basis.	Interview of resource proposed for SOC Manager	Maximum 02 marks
			Interview of resource proposed for Security administration and Threat Intelligence expert	Maximum 02 marks
			Interview of resources proposed for CSOC Engineer - 1.5 marks for each resource	Maximum 4.5 marks
			Interview of resources proposed for Level 2 analyst - 1 marks for each resource	Maximum 07 marks
			Interview of resources proposed for Level 1 analyst - 1 marks for each resource	Maximum 07 marks
Technical Presentation				
8	Quality of technical design, approach methodology, solution specifications	Technical presentation to be given by the bidder to OCAC. Marks would be awarded as per the technical committee of evaluation from OCAC.	Marks would be distributed as per the approach and methodology, past experiences and credentials presented by the bidder.	10 marks
9			Marks would be awarded as per superiority in terms of technical specifications and capacity of the solutions as proposed by the bidder.	10 marks

Note: Bidders have to obtain a minimum score of 70 marks in the technical evaluation for qualifying for the financial evaluation.

3.10.3 Financial evaluation

The Evaluation Methodology proposed to be adopted by OCAC will be Quality cum Cost Based System (**QCBS**) method of evaluation where Technical Bid Score will get a weightage of 70% (denoted by ST) and Commercial Bid Score a weightage of 30% (denoted by SF).

The process of selection of successful bidder for the purpose of award of engagement shall be as follow:

A. **Calculation of Technical Score (ST)**

T = Technical Marks Obtain by the Individual bidder.

TH = Highest Technical Marks Obtained by bidder.

ST = Technical Score obtain by the Individual bidder

Calculation of Technical Score (ST)

ST = 100 x (T/TH)

B. **Calculation of Financial Score (SF)**

F= Total Financial Bid amount quoted by individual Bidder

FL= Lowest Total Financial Bid amount quoted by individual Bidder.

SF = Financial Score obtain by the Individual Bidder

Calculation of Financial Score (SF)

SF = 100 x (FL/F)

C. **Calculation of Final Composite Score (S)**

The Final Composite Score (S) shall be computed for each firm by assigning 70% weightage to the Technical Score (ST) and 30% weightage to Financial Score (SF) using the formula given below:

S = (ST x 0.7) + (SF x 0.3)

Bidder with the highest final composite score will be awarded the engagement. In case of a tie in the final composite score, the bidder with the higher Technical Score will be invited for negotiations and selection first.

4. Scope of work for bidder

Cyber Security Operations Centre (CSOC)

The bidder shall supply skilled manpower for Cyber Security Operations Centre (CSOC) operations over a period of four years at OCAC location as detailed in this document. Implementation Agency shall ensure uptime & availability of all CSOC devices and tools. Service provider resources are expected to deliver SOC services including but not limited to performance monitoring, performance tuning, optimization, and maintenance of CSOC security tools, SIEM log backup, troubleshooting, security monitoring, security product management, vulnerability assessment and penetration testing and application security testing. The detailed SOC reports formats will be discussed and finalized with bidder.

The scope is limited to three stakeholders in the initial phase of the project:

1. Odisha State Data Centre (OSDC).
2. State Wide Area Network (SWAN).
3. State IT Centre.

Initially implementation of CSOC is to be carried out for the above three stakeholders. On reaching stability and maturity of CSOC system, additional stakeholders would be added to the project and the scope of work for the bidder would be expanded covering the additional stakeholders also. The bidder should propose cost for the project as per the format / proforma provided in the RFP document.

The selected CSOC implementation agency under this RFP would deliver services like:

Security Monitoring Services:
This service will help OCAC to monitor for security events throughout its network by analysis of logs from servers, devices and key applications.

The following security monitoring service will be catered by CSOC:

- Government department information security and monitoring.
- 24 X 7 security monitoring, detection, response and recovery.
- Real- time Threat intelligence, advanced correlation and proactive threat detection.
- Integrated cyber security/security framework.
- Monitor cyber-attacks, threats, intrusions, incidents for the critical infrastructure like SDC, SWAN and State IT Centre.
- Extend Security to all Critical Infrastructure of the State (e.g., SDC, SWAN, IT Centre, etc.).

Security Product Management:
This service will help OCAC to centralize the management of security products and to have tight control on the security rules. Services will also include security products procured in future. The services will include-

a. Configuration, fault, performance and availability management of the CSOC infrastructure.
b. Activities like but not limited to; patch management, firmware upgrade, configuration backup.

c. Co-ordination with internal teams for rule base management.

Vulnerability Management Services:
This service will help OCAC to centrally assess and mitigate the security risks in its network, servers & devices on a continuous basis. The service will include-

a. Set up a baseline security level for department assets.
b. Conduct VAPT and Application Security tests as in when required.
c. Bidder has to provide tools / utilities and skilled resources to conduct the respective tests.
d. The bidder's (SOC) team has to provide recommendations for closure of findings & provide reports on daily basis till closure.
e. Assess the current environment against baseline on periodic basis.
f. Ensure that the baseline is maintained on an ongoing basis and hence assets are secured against risks.
g. Track the mitigation and coordinate with asset owners for closure of security gaps.

All the services mentioned above are to be provided during the various phases of the project as given below:

4.1 Pre-Bidding phase

Site Survey

- All Bidders shall be required to survey the proposed CSOC control room site before the submission of the commercials.
- All the Bidders shall perform site-survey of all the project location followed by the preparation & submission of bid.
- The survey shall include the details of the location positioning and establishment of the CSOC.
- The cost of survey would be borne by the bidder. OCAC holds no responsibility on the cost undertaken by the bidder for site survey.

4.2 Implementation phase

i. Civil Construction and interior design as per standards.
To be done as mentioned in Section 5.2 and 5.3 of the RFP document.

ii. Site Preparation.
Site preparation structure for CSOC would include false ceiling, lighting, glass and gypsum / plywood partition, flooring, access control, fire safety and command centre furniture.

External civil construction may or may not be a part of the scope of the bidder, discretion of developments and future decisions of OCAC. The scope may be revised at a later stage with timely intimation to the bidder. Civil construction inside the identified CSOC space / area would be under the scope of the bidder.

iii. CSOC command centre design, installation and commissioning.
The successful bidder in coordination with OCAC shall arrange for necessary clearances including statutory and regulatory which shall enable them to undertake civil, electrical, and mechanical works including building

modification, partitioning, installation of electrical component, cable laying etc. at the CSOC site.

iv. Design, supply, installation, commissioning for IT and Non-IT Infrastructure for CSOC.

The successful bidder should carry out:

- Complete procurement, supply, installation and commissioning of required IT, Non IT, and civil infrastructure at all the designated locations of the CSOC as identified.
- Successful bidder shall submit stage-wise reports and it should be done strictly in accordance with the scope of work in the document.
- Successful bidder is expected to adhere to all technical and non-functional specification for IT, Non-IT and civil infrastructure.
- Any additional design guidelines as provided in the tender document / proposed solution document has to be achieved as per established delivery time lines.
- A detailed project plan for the implementation of CSOC is to be provided during the Kick-off meeting by the successful bidder.
- A work break down structure with all milestones for the entire commissioning time line is to be provided by the successful Bidder.
- The successful bidder would be required to submit detailed design documents with all necessary design drawings for all IT, Non IT and civil infrastructures and would be approved by OCAC Technical Committee before actual execution of work.
- A supply schedule for all materials with make and model is to be prepared and submitted in line with the work break down structure of the project plan.
- All materials are to be dispatched as per expected delivery time lines with no additional dispatch or delivery costs.
- Any deviation from the expected time lines of delivery is to be intimated in advance for appropriate actions and reason.
- The materials should be brand new and as per the tender specifications/requirements.
- Bidder should take care of Insurance against the material loss.

v. Integration of existing departmental and security IT infrastructure with the proposed CSOC infrastructure.

- All components of CSOC must support scalability with adequate licensing, accessories and modules to provide continuous growth to meet the requirements and demand of various departments.
- Bidder should analyze and study the current departmental infrastructure located at OCAC and Secretariat and provide the solution for migration.
- Bidder accordingly shall implement the solution provided for integration of all applications and hardware. The details regarding the current scope of integration with CSOC is given in Annexure – I of the RFP document.
- Necessary inputs would be provided by the respective application vendor and current Data Centre operator.

vi. Final Acceptance Testing (FAT) for IT and Non IT components under CSOC and CSOC Go-Live.

- FAT reports will be verified and approved jointly by OCAC, Consultant and successful bidder following which the commissioning certificate will be issued by OCAC. All Civil, IT and Non IT systems are to be installed and tested as per the tender and continuous status reports are to be submitted.
- Consultant and OCAC will participate in the active project management and monitoring of time lines to ensure adherence to delivering on schedule.
- Commissioning certificate will be issued by OCAC after completion of the project components as per scope of work.

4.3 Operation and Maintenance phase

1. On-site comprehensive maintenance and provisioning of services of all the ICT Infrastructure and their components supplied with a provision of onsite spares on 24x7x365 basis after successful execution and acceptance by OCAC.
2. Onsite support for CSOC Operations on 24x7x365 basis by qualified and trained personnel for a period of four years to ensure high service availability.
3. The successful bidder should provide 24 x 7 x 365 operating and maintaining services for a period of 4 years from the date of Go Live for CSOC.
4. The successful bidder is required to provide the comprehensive onsite maintenance with part replacement for all the IT and Non IT equipment.
5. The successful bidder shall be responsible to ensure adequate and timely availability of spare parts needed for repairing the equipment/ parts.
6. To provide this service the selected bidder must have back to back arrangement with the respective OEMs/ OEMs authorized partner.
7. The successful bidder has to make necessary arrangements of spares for catering maintenance needs of equipment/parts during entire engagement period at no extra cost to the client.
8. Root Cause Analysis of the incidents (Major & Minor) to identify threat sources and proactive measures to prevent recurrence.
9. Successful bidder will be responsible to store logs in industry standard solution and format for extraction and sharing with other solutions/ agencies.
10. Analysis of SIEM logs to identify information security vulnerabilities in environment and provide recommendations to prevent these vulnerabilities.
11. Reporting and logging of all security incidents through the use of appropriate ticketing tools. Track and monitor the closure of these information security incidents and escalation of these incidents to appropriate teams/ individuals.
12. The successful bidder shall also provide a detailed process for managing Incident Response (IR) describing each phases of the process – prepare, identify, contain, eradicate, recover and learn from the incidents responded to.
13. Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact.
14. The services and solutions in scope should be designed with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime and availability.
15. Preparation of CSOC SOPs and User manuals, BCP plan, Exit Management Plan, Helpdesk management, Change Management, etc. documents.
16. Training to OCAC officials (designated by OCAC) and upgradation of CSOC personnel on IT infrastructure, SLA management, various CSOC related polices, etc.

17. Engage at least 15 personnel from OCAC / department for the training sessions. Feedback of each attendee to be taken and shared with OCAC.

The scope of work during the operations phase is divided into following areas which are listed below:

- Administration, Maintenance and Management Services.
- Documentation related to Standard Operating Procedures (SOP), User manuals, etc.
- Backup & Restore Services.
- Physical Infrastructure Management and Maintenance Services.
- Preventive Maintenance Services.
- Corrective Maintenance Services.
- Asset Management Services.
- Configuration/ Reconfiguration Management Services.
- Vendor Management Services.
- Vulnerability Management services.
- Threat Management.
- Intelligence feeds.
- Global Threat intelligence subscription.
- Update management (patch update for all software and appliance possible).

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

Implementing agency shall provide trainings to department personnel regarding the operations and awareness of the security technology established in CSOC. The department would nominate personnel to undertake the training sessions and maybe in future the trained personnel coordinate in the CSOC related activities.

4.4 Partial Acceptance Test (PAT)

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

Partial Acceptance Test will be conducted by the Consultant / PMU in accordance with the timelines, scope of work as mentioned in the RFP and the solution documents proposed by the successful bidder and accepted by OCAC.

The Consultant / PMU will prepare and submit the report of PAT to OCAC and subject to its acceptance, it shall be deemed as completion of Partial Acceptance Test (PAT).

4.5 Final Acceptance Testing (FAT)

The acceptance of the Data Centre including DC site in accordance with the requirements shall be conducted. After successful testing of the features, facilities, functionalities and integrity of the commissioned devices, equipment and services by OCAC jointly with Consultant / PMU and successful bidder, a Final Acceptance Test (FAT) Certificate shall be issued by OCAC to the successful bidder.

The test shall include the following:

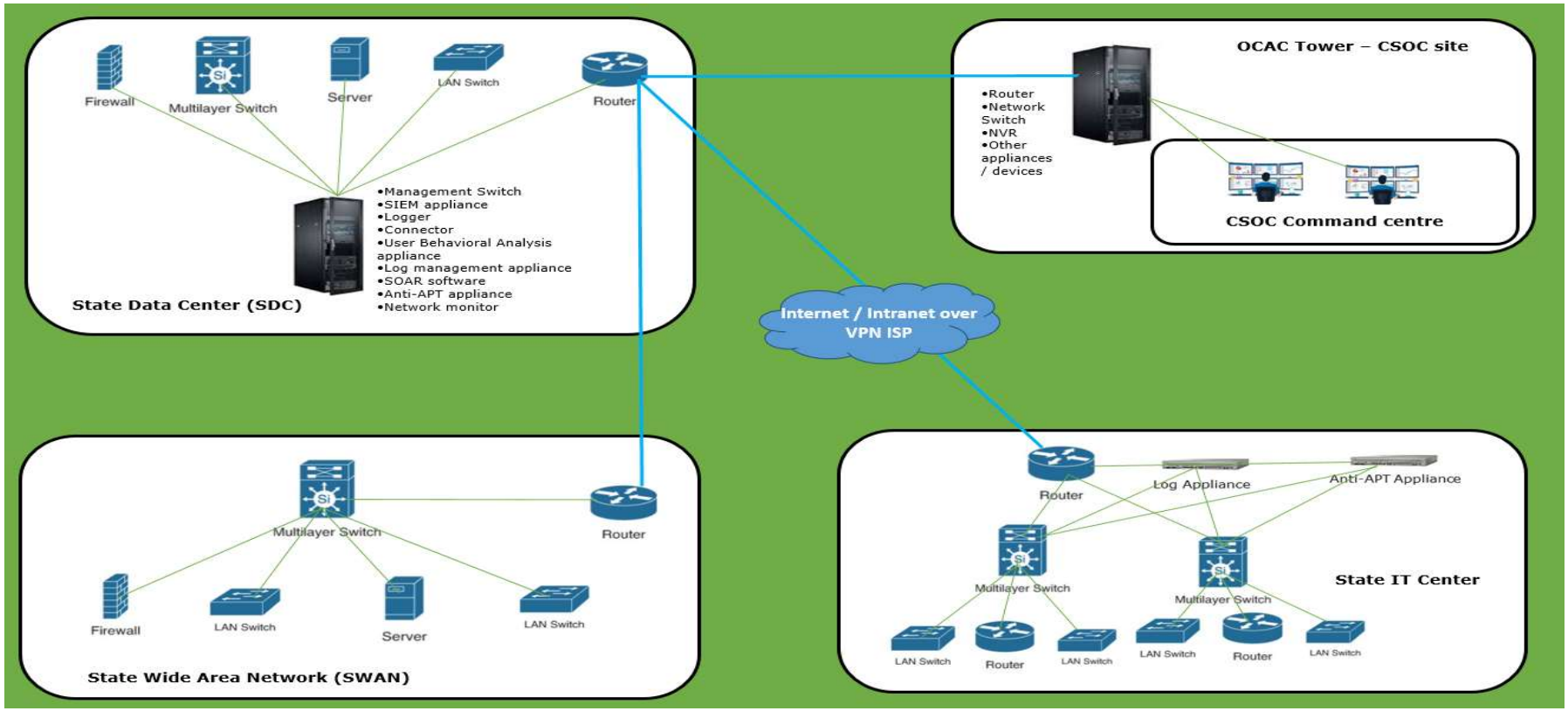
1. All civil, electrical, air conditioning works, etc., are completed as per the RFP specifications and solution documents proposed by the successful bidder and accepted by OCAC.
2. All hardware and software items must be installed at CSOC site as per RFP specifications and solution documents.
3. Availability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

5. Project Design

5.1 Project high-level architecture

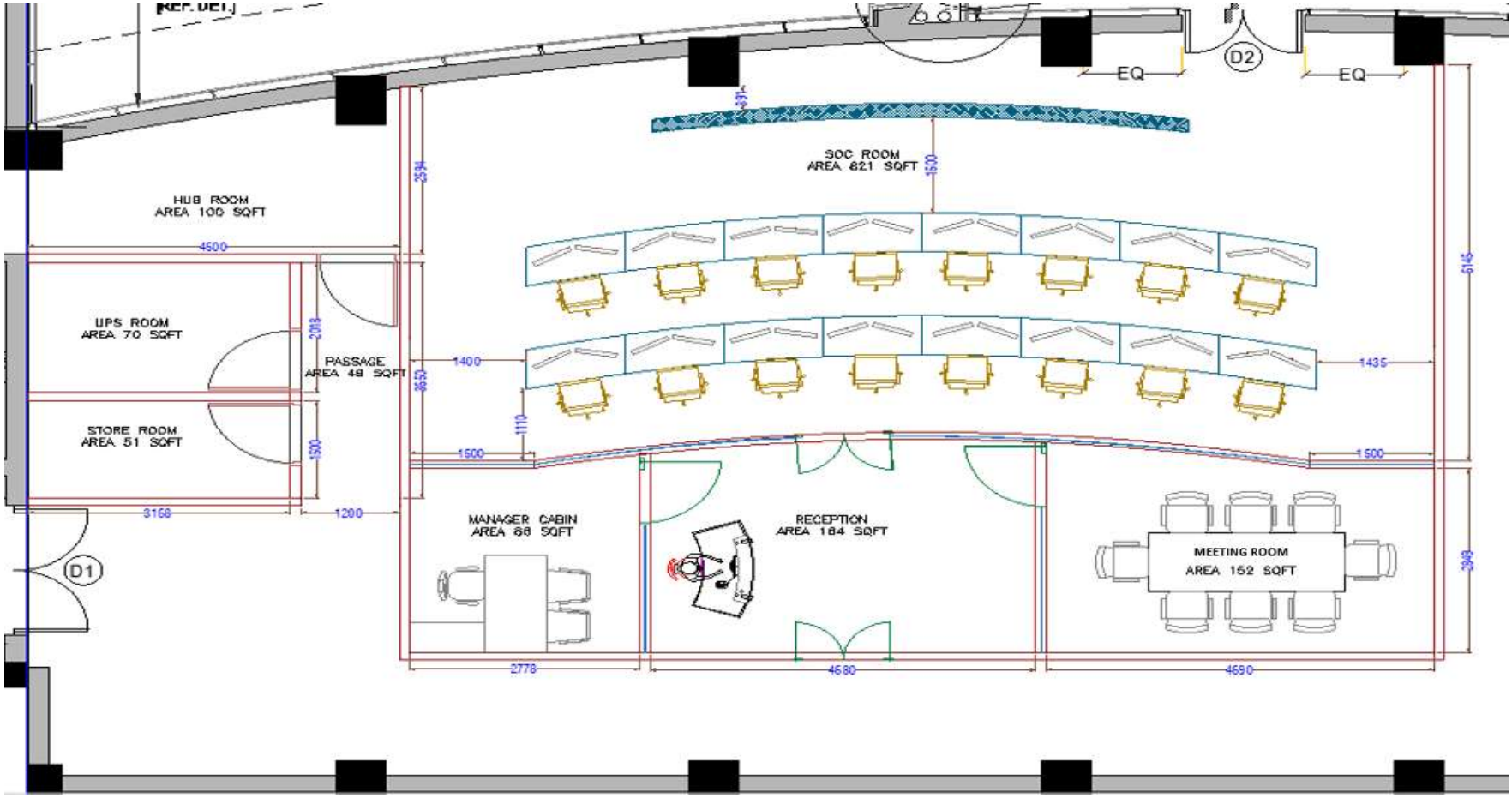
The current stakeholders in the project are:

1. Odisha State Data Centre (OSDC) – on same premises.
2. Odisha State Wide Area Network (OSWAN) – on same premises.
3. Odisha State IT centre – on distant premises.



5.2 Site layout

The CSOC site would be prepared as the specifications provided at First floor, OCAC Tower, Acharya Vihar, Bhubaneswar, Odisha. The suggested floor layout to be implemented by the successful bidder is given below:



Note:

1. The above layout is indicative only and may be subject to change. The bidders are advised to visit the site for clear understanding of the actual conditions before bidding.
2. The floor design given is indicative and bidder may propose more optimal design solution which would be subject to review and approval by OCAC.
3. The bidder shall disconnect the existing fire suppression system from the site in coordination with OCAC and site authority.
4. The bidder should install proper signage and cautionary stickers wherever required in CSOC premises.
5. The bidder should propose for glow signage for emergency exits and room / command centre indicators and entrances of Odisha CSOC site.
6. The bidder has to carry out any civil construction as required at the site for building up Odisha Cyber SOC.

5.3 Site Design

The bidder shall provide detailed design, documentation, make, and model, efficiency including user, system and operation manuals along with the necessary diagrams, design drawings and details bifurcation of Bill of Materials (BOM) along with detailed description. The site drawing (to be submitted before execution or as on when required) may include but not limited to the following:

- Site layout
- Equipment placement layout
- All drawing for Electrical scheme including single line diagram
- All GA drawing of equipment
- Grounding and Earth pits
- Lighting
- Furniture placement
- Networking cabling
- Trenches, cable trays and raceways
- Aspirating smoke detection, water leak detection, rodent repellent, CCTV, access control system
- Sectional views
- SOC command centre console / table
- 3D drawing as required.

As and when required, the successful bidder has to submit the coordinated drawing for the solution. The bidder shall take the necessary clearance / approval of the drawings, design, quality of material, make and model of the quoted material etc. prior to the execution of the project.

After implementation of the civil works, the bidder has to obtain relevant certifications for the site and share the same with OCAC.

5.4 Site Civil & Non-IT works

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

FLOORING

1. False flooring for Command Centre:

Providing and fixing bare finish false flooring with steel cement tile, made out of high grade cold roll steel sheets, of size 610 x 610mm size, in 30mm thickness. Top & bottom plate joint with 100 spot welding & cavity is filled with light weight cement for solid load baring capacity, coated on all sides with epoxy powder coating for long life. These tiles should be placed on to the steel under structure pedestal at required height. The product should be fire rated non-combustible material. The system should be fully access able with changeable panels on any direction required, complete in all respect including cost of materials, labour etc. This should have load bearing capacity of 1650 kg/ sq.m Height up to 600 mm. All measurements in multiples of 300mm. In case tile is cut into curve, cut tile will also be measured. Tile puller - Double cup.

Step for false flooring: Providing and fixing of Step made up of 50x25mm aluminium sections cladded with 2 nos. of 19mm ply / flexi ply / bison board coated with fire retardant paint. To be finished with laminate as per approved design. In straight or

curved shape. L shaped aluminium extruded Edge profiles at the edge of the step / level difference. Edge profile edge should be rough to avoid the slip.

The edge profile shall have LED light in desired colour at the steps where movement is expected.

2. Italian Marble / Composite stone Flooring:

Providing and laying 15-20mm thick stone of approved shade and colour as per design patterns and with appropriate slopes shown on the drawings laid on white cement mortar bedding of 1:4 of average thickness up to 25mm laid o on grey cement slurry inclusive of cutting, curing and finishing of joints with colour pigments. Rate to include diamond polish, as per desired finish. The rate quoted shall include for keeping the laid flooring protected with Plastic Sheet & POP till handing over and cleaning the same.

3. Carpet Flooring:

Supply and installing 500mm x 500mm or 300mm x 1200mm carpet tiles with secondary backing of P.V.C The rate shall include cutting, trimming, fixing and clearing away of residual material to a location as directed. The rate shall also include supplying and laying of a protective layer of PVC sheet of 50 microns thickness, held together with scotch tape. The laid carpet to be vacuumed after the removal of protective cover/on commissioning. In case the stains are observed in the carpet after the protective layer is removed, because of inadequate protection, the same shall be shampooed and made good to the satisfaction of the project managers.

PARTITIONS AND PANELLING

Partition / Panelling - Curved Or straight at different levels to create trough for hidden lights

Aluminium / GI frame at 600mm x 600mm c/c with additional supports at strategic locations and filled with acoustic sound absorbent material of high density wrapped in tissue paper and finished with following materials:

i. 12.5mm thick gypsum board
ii. 12mm Bison board / ply / MDF and finished with laminate
iii. 12mm MDF, covered with CNC cut designed panels and finished with Duco paint
iv. Acoustic panels in various shapes and sizes and covered with fire retardant fabric to give 0.9 NRC
v. 8mm thick ply backing and finished with 6mm thick lacquered glass in desired colour
vi. Full Ht. 2 hours Fire Rated Gypsum Partition: Form full height partitions with GI sections at 600 mm distance. Partition frame to be faced both sides with 2 nos. of 12.5mm thick fire & moisture (RFMR) gypsum board. OEM specifications shall be followed. Partition shall be finished with jointing tape / compound etc. HUB/ UPS Room/Battery.
vii. Designer CNC cut metal panelling P/F of designer CNC cut in desired shape metal wall panelling in desired colour including base frame.
viii. P/F fully glazed partition of 10mm thick toughened float glass fixed with 45x25mm Black Alloy frame in floor/wall complete in all respect as per detail drawing and as directed by architect. The joints between glass panels are provided with Aluminium I section.

Designer Printed Film: Opaque / semi opaque film to be installed on clear glasses per the design reference image. Quote should include cost to prepare ready to print design.

Wall Graphics: Supply and applying approved Graphics as per manufacturer's specification. Surface preparation - thoroughly sand papering surfaces to remove dust, dirt, etc., and repairing dents, holes with POP to achieve level surface and finishing including cost of material, labour, scaffolding etc., all complete.

i. Wall paper on top of existing POP finish wall / gypsum partition.
ii. Corner guard in Anodized / desired powder coated finish 25x25mm fixed on all exposed corners with adhesive.
iii. P/fixing of 300mm laminated window sill made of aluminium framework + 19mm thick ply + 1mm thick laminate on existing window sill complete in all respect as per detail drawing, specification and as directed.
iv. 50mm high aluminium skirting- Providing and fixing 1.5 to 2mm thick 50mm high extruded anodized aluminium skirting fixed over wall / partition including cost of 12mm ply backing if required.
v. Providing and applying Plaster of Paris punning on walls for true level.
vi. Putty on wall to make it smooth. Applying putty on walls & columns surfaces to make it ready to receive paint.

PAINT

Applying premium plastic emulsion paint on false ceiling/walls three or more coats with roller I/c applying cement primer, making smooth surface with putty to the satisfaction of architect or smooth base to fix the wall paper / graphic. Providing and Applying Duco paint in approved colour with Duco primer, making smooth surface with putty. The surface on finishing shall present a flat velvety smooth finish. If necessary more coats will be applied till the surface presents a uniform appearance.

DOORS

i. Fully glazed frameless glass door of 12mm thick toughened Modi /Asahi float glass with single or double action heavy duty floor springs and SS patch fittings hinges, lock, provision for electronic lock for access control, 1200 mm long SS Handle complete in all respect as per detail drawing and as directed by architect. Cost should include demountable door frame with groove all around.
ii. Fire Door for UPS and Server room: Made of GI with powder coating in desired colour and inclusive of all hardware accessories and there should be a provision of 300x300mm fire rated viewing glass window.
iii. Providing and fixing 250 to 300mm deep laminated openable shutters for electrical panel made of 19mm thick (Phenol formaldehyde bonded BWR grade) board; boxing, partitions, shutters with external surfaces to be cladded with 1mm thick laminate with teak wood moulding including and enamel paint on internal surfaces with all hardware, locks etc.

The doors requirement is given in the table below:

Sr. No.	Door details	Type
01	Main entry door to facility from corridor side	Double leaf glass door of total 2000mm width
02	Entry to command centre from east side	Fire rated glass door in SS 304 frame

Sr. No.	Door details	Type
03	Entry to Network / UPS area from corridor	Fire rated steel door (min 45mm thick and 1200mm width) with vision glass
04	Store room, Network room and UPS room	Fire rated glass door in SS 304 frame
05	Manager and Meeting room area	1200mm toughened glass door and glass partition

The above list is indicative only & the bidder may propose additional doors of desired specifications if required as per the actual site conditions. There will be designer privacy film on every glass door. Bidder may decide to erect/not erect wall as per requirement of their design.

FALSE CEILING

The false ceiling for the CSOC site can be a designed as a mixture of metal baffle, acoustic, curvilinear and printed ceiling. The design to be proposed by the bidder.

1. Metal Baffle Ceiling:

Baffle Ceilings should be Extruded Aluminium / GI profile of 1.2mm thick and of size 25mm x 100mm. The Baffle panels are coated with wooden / solid colours of approved wood finish. The baffles are connect to tailor made baffle "C" Carrier of 1.2mm thick and with slots as per spacing's required between each baffle panels at 125mm centre to centre. The baffle panels are connected with the baffle carrier with bolt/nut/spring washer arrangement thereby achieving a firm connection between them. The baffle "C" Carrier is then suspended at every 1mtr with 6mm threaded rod, where one end is connected to the carrier and the other end with anchor fastener fixed on true ceiling. The baffle panels come at a maximum size up to 5.8mtr. in length. The baffle end with an End Cap is made in Aluminium and is with same finish as the baffle panel. Wherever required two baffle panels are connected by a splice to make it run continuously or with a gap of 20mm as per requirement.

2. Designer Acoustic False ceiling:

Mineral Fiber /Glass wool based Acoustical Suspended Ceiling System with tegular edge tiles with exposed silhouette grid. The tiles should have Humidity Resistance (RH) of 95%, NRC 0.9, Light Reflectance >85%, Thermal Conductivity k = 0.052- 0.057 w/m K, Fire Performance Class1 or A as per ASTM E 84, suitable for Green Building application, with Recycled content of 63%, tile size can be 300x1200 or 600x600 mm in DESIRED colour as per the design.

3. Curvilinear / designer (in varying shapes):

12 mm gypsum board false ceiling with level adjustor (flat/tapered, vertical) The ceiling should be finished to get true line & level The ceiling should be braced to wall /windows framing where blinds/curtain boxes.

4. Ceiling Access Door:

Bidder has to supply & install Access/Trap doors made of cementitious board and finished with the laminate. Size shall be as per the design requirement.

FURNITURE

1. Control Desk (H x W x D = 750mm X 9478mm X 900 / 1050 mm)

i. Console desk for 8 users with provision of placing 16 Nos. of monitor on Monitor Mount, 8 Nos. of keyboard/Mouse on Sliding Tray.
ii. Table design should be fluidic in nature and should be futuristic
iii. Table top finish should be Acrylic moulded (Corian) in desired colour and shape.
iv. Provision for hidden lights including LED lights should be considered
v. Adjustable dimmable task light should be provided in desk
vi. Wire Managers - For routing LAN & Power Cables within the Table.
vii. Adequate Heat management provision for Exhaust of heat from within the desk Assembly.
viii. Power Distribution Sockets - within the Table for Powering of Active Devices.

Structure

Console System must be of modular design. The Console design shall address the functional, ergonomic and aesthetic requirements of the particular working environment while complying with accepted human factor design and ergonomic standards for viewing distance, angle, keyboard, height, and knee space requirements.

- Standard top height of modular control desk shall be 750 mm. The Console Table Top / Working
- Surface should be made of 18mm MDF Board with 12mm Solid Acrylic Panel.
- The Basic Structure should consist of Extruded AL Profiles (6063T6 grade) binded by Top & Bottom (min 2mm) MS Frames formed in such a way as to provide maximum buckling and torsion resistance. The Front & Back Panels should be openable / removable (with Push Lock Mechanism) made of laminated MDF Board in min thickness of 18mm. The Side Panels should be fixed type, made in 26mm MDF Board Cladded on 18mm MDF Board. All panels must be attached to the frame with concealed fasteners. Console access panels (Front & Rear Panels) must be removable without the use of tools. The Front panel should be positioned in such a way that there should be sufficient leg space (min of 400mm from the front edge of the Table Top).
- All sheet metal / aluminium parts must be finished with electrostatic powder coating with average of min 80 microns over all surfaces.
- The console frame shall have provisions for leveller legs to be incorporated into the frame.

Work Surface

The Console Table Top should be made of 18mm MDF Board with 12mm Solid Acrylic Panel. The work surface platform shall have smooth edges and transitions, thus avoiding sharp corners or potential rib catchers for operator safety.

Modular Rear Wall (Slat Wall)

- Wall should be of min 86 mm (Height) and approx. 200-300 mm high from the Monitor Base.
- Modular walls shall be made of 2mm thick Extruded Aluminium (6063T6 aluminium alloy).
- It should have high Load bearing capacity. Minimum weight carrying capacity has to be 20 KGs per Meter.

Monitor Arms

- It shall be capable for mounting all type of existing LCD monitor with dimensions between 19" to 27" using suitable adopter/additional base plate, if required any.
- Vendor shall provide the suitable adopter/additional base plate for mounting the existing LCD monitors.
- It shall allow the rotate/ tilt/ raise/the monitors as well as fix their adjustment.
- The monitor arm should be Articulating monitor arm.

Miscellaneous

- There shall be a closed cabinet below the modular control desk for placing of CPU. Cabinet should have proper cooling system. CPU needs to be accessible from front as well as rear side of control desk for easy working and maintenance.
- The cabinet shutters shall be of Butt Hinged type with 18mm thick MDF.
- Rear shutters of each console should have provision of Airflow opening for cooling and heat dissipation effect.
- Rear panel shall have ventilation fans mounted on it.
- Hidden LED lights to be provided for Aesthetics.
- Adjustable Dimmable LED Light to be provided on the Desk.
- It shall have proper arrangement for flow of cables i.e. LAN Cable, Power cable, VGA cable, Mouse cable, Keyboard etc.
- Design of control desk shall allow cables from the floor cable channel.
- Control desk shall be equipped with individual power distribution unit (PDU) (06 no for one Modular Control Desk) and capable of being switched on/off individually. Power supply socket should be dual type i.e. Universal type.
- All bolts must be of SS material to avoid rust due to environment.

Bidder should submit the below certificates / documents after the completion of control desk / console:

a) ANSI / BIFMA Certificate for Consoles
b) ISO 9001, ISO 14001 & OHSAS 18001 Certificate
c) Green Guard Certificate for low emissions
d) ROHS Compliance
e) ASTM E84

2. Manager Table (H x W x D = 750mm X 1800mm X 800mm)

i. Manager Table with provision of placing 1 Nos. of monitor on Table Top, 1 Nos. of keyboard/Mouse on Sliding Tray.
ii. Made of 40mm thick Laminated MDF top, powder coated metal / 25mm laminated MDF under structure, metal / laminated Mdf modesty as per the client choice
iii. Side storage of 750mm x 1050mm x 400 mm should be provided
iv. MDF Based Drawer Unit with all sides laminate. Laminated 18mm (±1mm) MDF Board Construction
v. Wire Managers - For routing LAN & Power Cables within the Table.
vi. Adequate Heat management provision for Exhaust of heat from within the desk Assembly.
vii. Power Distribution Sockets - within the Table for Powering of Active Devices.

3. Meeting Room Table (H x W x D = 750mm X 2700mm X 1050mm)

i. Made of 40mm thick Laminated MDF top, powder coated metal / 25mm laminated MDF under structure as per the client choice
ii. Wire Managers - For routing LAN & Power Cables within the Table.
iii. Adequate Heat management provision for Exhaust of heat from within the desk Assembly.
iv. Power Distribution Sockets - within the Table for Powering of Active Devices.

4. Reception Table (H x W x D = 1000mm X 1500mm X 700mm)

i. Table design should be fluidic in nature and should be futuristic
ii. it should have double level
iii. Top, front and side finish should be Acrylic moulded (Corian) in desired colour and shape.
iv. Provision for hidden lights including LED lights should be considered.
v. MDF Based Drawer Unit with all sides laminate. Laminated 18mm (±1mm) MDF Board Construction.
vi. Wire Managers - For routing LAN & Power Cables within the Table.
vii. Power Distribution Sockets - within the Table for Powering of Active Devices.

5. Command centre chair / Meeting room chair / Visitor Chair / Manager chair

Command centre chair must ergonomically designed in such a manner that long hour seating does not become tiring. The preferred requirement of chair are: Mid Back Chair, for Manager High back, Mesh Back & Silver Epoxy Backbone, Synchronized Mechanism, 4-Way Adjustable Armrest, Seat height adjustment, Standard 5-prong P/Nylon Base, BIFMA & GREEN GUARD certified.

6. Shoe Rack

A shoe rack must be supplied with 16 pair of slippers to be placed at the allocated area as per site layout.

7. Sofa set with coffee table

Sofa set with suitable coffee table shall be supplied for the reception area as per design and layout for the CSOC site. Sofa should be of modern design and finished in leather. Coffee table should be (H x W x D = 450 mm X 1050mm X 600mm) modern design and 10 mm toughened Glass Top.

8. Staff locker

The locker should be made of steel, of standard design as per storage locker. Each individual locker dimensions should be approx. (Depth x Width x Height) 40 cm x 40 cm x 45 cm. The locker should be painted, powder coated, polished and corrosion resistant. Each locker should have facility for pad locking. Each locker should have facility for name tagging. 16 nos. of lockers should be available in total for the CSOC staff.

9. Storage Units

The storage should be made of hard plywood. The dimension of the each unit should be at least (L x B x H) 90cm x 60cm x 120cm. Each unit should have hinged doors of equal width hung with auto closing hinges of 0 cranking overlay type. The hard plywood should be at least 20mm thick. Each unit should have at least four number of shelves. Each unit should have lock and key facility. The color of each unit should be moderate and suitable with the background of the premises.

ELECTRICAL

i. Supply, storing, handling, laying, testing and commissioning of 1100 Volt grade XLPE insulated and sheathed aluminium conductor armoured cables, ISI marked , including providing required gap between adjacent cables (minimum one cable dia.) including providing identification tags in shaft/ cable trays etc. complete as per specifications, as required (Low v/d losses).

ii. Supply, storing, handling, laying, termination, testing and commissioning of 1100 Volt grade XLPE insulated and sheathed copper conductor un-armoured cables ISI marked including providing required gap between adjacent cables (minimum one cable dia.) including providing identification tags in shaft and cable trays in ground etc.

iii. Supplying of all materials and making end terminations of 1.1 KV grade XLPE insulated aluminum multi core cables of the following sizes. The work includes cable cladding using brass plated double compression glands, sizing the core leads, removing insulation, fixing suitable crimping type heavy duty aluminum lugs/ thimbles by using hydraulic crimping tools with correct size of the dies, shaping the leads and neatly connecting the same to the equipment terminals.

iv. Supplying of all materials and making terminations of 1100 Volt grade PVC insulated and sheathed copper conductor unarmored cables including providing required gap between adjacent cables (minimum one cable dia.) and the cost of providing identification tags in shaft/ cable trays/ in ground etc. The work includes cable cladding using brass plated double compression glands, sizing the core leads, removing insulation, fixing suitable crimping type heavy duty copper lugs/ thimbles by using hydraulic crimping tools with correct size of the dies, shaping the leads and neatly connecting the same to the equipment terminals.

v. Supplying and installing following size of perforated Hot Dipped Galvanized Iron cable tray (Galvanization thickness not less than 50 microns) with perforation not more than 17.5%, in convenient sections, joined with connectors, suspended from the ceiling with G.I. suspenders including G.I. bolts & nuts, etc. as required.

vi. Supply, fabrication, erection & epoxy painting of steel items as required as per specification complete, Generally steel items include cable tray, cable tray supporting arrangements, MS Channels-(ISMC), Angles, Plates and any other steel items not covered in other items of schedule of quantities. The cable trays shall be of ladder made of angles and flats / sheet steel folded type. The rate shall also include painting with two coats of red oxide and primer and two coats of synthetic enamel paint of approved shade.

vii. Factory Fabricated wall mounted distribution board with one incomer of 160A 4P MCCB, Cu Bus bar, MFM, and outgoing MCB for UPS and other DBs.

viii. 8 Way TPN DB with One No. 63 A FP MCB as Incomer and Twenty Four No 10/20 A SP MCB as outgoing. (Light /Power DB).

ix. 8 Way TPN DB with One No. 63 A FP MCB as Incomer and Twenty Four No 10/20 A SP MCB as outgoing. (CAC DB).

x. Supply, store, erection, testing and commissioning of factory made metal clad totally enclosed with cast aluminum housing with industrial socket/interlocked combined rotary switch and socket with scrapping earth connection and plug top. In case of interlocked socket, the interlocking should ensure that the plug cannot be inserted or withdrawn while the switch is in 'ON' position (all switches & sockets shall be housed in painted MS boxes). The erection rate shall include supply of angle iron

frame work and fixing accessories such as grip bolts/grouting/ welding to steel structures etc., All the MCBs shall be of 'D' Curve specifications.

xi. MCB shall comply with IS/IEC 60898-1 2002 and IEC 60947-2 or as per revised standards. The terminals in DB shall be protected against any finger contact to IP20 degree of protection. All the MCB units shall bear ISI & CE mark and breaking capacity should be 10kA.

i. Supply, erection, testing and commissioning of power points by providing switches / sockets mounted on suitable size metal coated boxes fixed flush/surface on to the wall with all fixing and wiring accessories.

ii. Normal power: 6/16 Amps, 3-pin (250 Volts) single phase universal socket with 16 Amps single pole switch with indicating lamp. The pin configuration shall be round type.

iii. Safety and Security systems UPS Power: 6/16 Amps, 3-pin (250 Volts) single phase universal socket with 16 Amps single pole switch with indicating lamp. The pin configuration shall be round type. Plug tops are excluded from the scope of supply.

LED Ceiling lights

i. General Lighting Solutions which offers excellent energy saving and maintenance free operation. The luminaire should have slim design, which is suitable for recessed mounted application for control room. The light output should be diffused and should not create any glare on the screens. This should consist of 600x600 / 300x1200 size or any other size as per design requirement.

ii. Circular shape down lighter LED fitting with all accessories.

iii. Dimmable lights for control rooms, dimmable down lighters with high system efficacy, Power Consumption 12W to 24W, highly efficient constant current LED drivers. Cost to include Dimming Lighting Dali Master Controller, dimmable drivers and Touch Panel.

iv. Dimmable linear lights including Aluminium cover and acrylic bottom for baffle ceiling in control room.

v. LED strip lights for the coves. This should be of a higher wattage and should be in desired colour / able to change colours.

AIR CONDITIONING

The bidder should to visit the site prior to bidding to assess the air conditioning input duct and dimensions to plan propose likewise. The bidder is required but not limited to perform the following activities:

i. Supply and Installation of AC duct work from the AHU mouth for the entire area of SOC.

ii. Linear grill, Diffuser (ceiling mounted) for return air.

iii. Any other works as per design and operations requirement.

6. Minimum technical requirement (Non - IT assets)

6.1 Earthing

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

6.2 UPS

Sr. No.	Component	Requirement description
1.	Functionality	Supports extended battery bank capacity
2.		Alarm indicator present for on battery / mains, overload, battery fault, trip, main fault, etc.
3.		Relevant certificate of quality assurance from reputed bodies or associations: IEC/EN 62040-1-1 "General and safety requirements for UPS used in operator access areas." EN 62040-2 "Electromagnetic compatibility (EMC) requirements" IEC/EN 62040-3 "performance requirements and test methods
4.		Independently controlled maintenance bypass
5.		Capable to be turned off without any interruption to power supply to devices.
6.		The proposed UPS should be Transformer free design, Full IGBT double conversion Technology.
7.		UPS should be of N +N configuration. Battery back up to be provided for 60 minutes on each UPS at Full Load.
8.		UPS system should be capable of operating in synchronization mode with similar rating of UPS. Design of UPS should be Insulated-gate bipolar transistor (IGBT) rectifier
9.		Each UPS should have phase sequence correction kit without switching in to battery mode as a default feature.
10.		Linear load harmonics distortion should be less than 3% and non-liner load harmonics distortion should be less than 5%.
11.		Efficiency of UPS should not be less than 95%
12.		Noise generated by UPS under normal steady state condition should not be more than 60 dB.
13.		UPS should be ROHS complied product.

Sr. No.	Component	Requirement description
14.		The type of battery shall be VRLA batteries with combination of LMO & NMC (Lithium Manganese Oxide & Nickel, Manganese, and Cobalt).
15.		Battery would be sealed and maintenance free type (SMF).
16.		The UPS Module would have the battery circuit breaker mounted near to the batteries. When this breaker is opened no battery voltage would be present in the enclosure.
17.		The battery breaker would be automatically disconnected when the battery reaches to minimum discharge voltage level or when signaled by other control functions
18.		The batteries would be housed in suitable Racks.
19.	Technical specification	Minimum load of 20 KVA
20.		IGBT based
21.		Minimum power factor of 0.8
22.		Input power: Three phase 300 V - 450V sinewave,50Hz
23.		Output power: Single phase 230V +/-1% sinewave 50 Hz
24.		Minimum 60 minutes back-up on full load
25.		Minimum output voltage of 400volt
26.		Static Bypass: The static bypass shall be used to provide transfer of critical load from the Inverter output to the bypass source. This transfer, along with its retransfer, shall take place with no power interruption to the critical load. In the event of an emergency, this transfer shall be an automatic function.
27.		Maintenance Bypass: The system shall be equipped with an external make-before-break Maintenance Bypass Cabinet (MBC) to electrically isolate the UPS during routine maintenance and service of the UPS. The MBC shall completely isolate both the UPS input and output connections.
28.		Paralleling Operations – The output of all the UPS systems would be directly connected at the load distribution panel through individual circuit breakers (part of the distribution panel). The load at the output would be shared equally by all the UPS systems. The paralleling control mechanism would be available with individual UPS. There would not be any single point of failure which can lead to collapse of all the UPS systems.
29.		UPS Batteries should be compliant to Safety Cell UL1642, Module UL 1973, Transportation UN38.3, Seismic GR63, EMC IEC61000-6-2, and 61000-6-4.

6.3 Closed circuit television (CCTV)

Sr. No.	Component	Requirement description
1.	Functionality	Type of camera should be dome, ceiling fixed, unidirectional.
2.		The camera should support rugged, indoor and vandal-resistant
3.		Should support IP configuration
4.		Should have day and night monitoring capability
5.		Should have alarm system with one digital input and two relay output and pre/post alarm buffer
6.		Should have multilevel user id and password
7.		Should support IP address filtering
8.		Should have auto exposure level control

Sr. No.	Component	Requirement description
9.		Should support good white balance indoors
10.		Should have auto gain control
11.		Should support backlight correction
12.		Should support remote administration for configuration and updates
13.		Should be accessible through a PC client / web client, onscreen display in English
14.		Should have digital signal processing
15.		Camera body should be of plastic with minimum IP53 protection with weight not more than 50 grams
16.		Suitable for operation from -20 to 50 degree Celsius
17.		BIS Registration for safety general requirements as per IS 13252 (Part 1):latest
18.		Should support connectivity and power over PoE.
19.		**NVR:**
20.		Should have high decoding capability for Full HD viewing and recording.
21.		Should have capability to view 16 channels simultaneously with synchronized real time playback.
22.		Should be equipped with quad-core embedded processor and operating system.
23.		Support 16 channel alarm input and output channels.
24.		Supports recording of video clip and storage.
25.		Capable of transferring recorded video / stored video to external storage device through USB or network.
26.		Should be capable of splitting the screen into 1/4/8/16 displays.
27.		Should have in built search feature as per time, date, exact and smart search.
28.		**PoE Switch**
29.		Up to 16 IEEE 802.3af / IEEE 802.3at devices powered
30.		Rack mountable
31.		Supports PoE Power up to 25 Watts for each PoE port
32.		Auto detect powered device (PD)
33.	Technical specification	Image sensor type: CMOS
34.		Image sensor size: 1 inch
35.		Picture mode: 3MP
36.		Resolution should be: HD (1280 x 720 Pixel),Full HD (1920 x 1080 Pixel) configurable into any one
37.		IR illumination range should be at least 50 meters
38.		Lens type should be fixed with variable focal length from 3mm to 8mm lens
39.		Focus mode should be auto / one push / zooming
40.		Frame rate should 30 fps
41.		Should support video compression: H.265,H.265+,MJPEG,MPEG4
42.		Should support dual compressed video streaming
43.		Should support 10x digital zoom and 20x optical zoom
44.		Should support vertical tilt range from 0 to 5 degrees
45.		Should support one way audio streaming with G.726, G.722.1, G.711 compression
46.		The camera should have UL Listed or CE Certified.
47.		Encrypted data transfer through HTTPS (SSL/TLS)
48.		Minimum lux to capture color image should be 0.5 lux
49.		Signal to noise ratio should be in the range 50 to 60

Sr. No.	Component	Requirement description
50.		Maximum shutter speed of 1/10000
51.		Support protocols: UDP, SNMP, IGMP, DHCP, RTP, RSTP, HTTP, SMTP, FTP, ICMP, HTTPS, DNS, DDNS, RTSP, RTCP, NTP, UPnP, QoS, TCP/IP
52.		Any additional PoE adapters if required without any extra cost.
53.		**NVR:**
54.		Should have minimum internal storage of 8 TB and expandable up to 32 TB.
55.		Support up to 16 channels H.264 / H.265 / MJPEG / MPEG4 compression and decoding.
56.		Should have one channel audio input and output.
57.		Should have minimum 2 HDMI, 2 USB, 1 RS232 and 1 VGA port.
58.		Capable of frame rate of 1-30 fps, bit rate approx. 20 Mbps per channel
59.		Support scheduled, manual, continuous, etc. mode of recording.
60.		Supports playback function of play, pause, stop, rewind, next file, previous file, etc.
61.		Support protocols: HTTP, TCI/IP, IPV4, IPV6, UDP, SMTP, NTP, DHCP, FTP, IP search, P2P, RTSP, etc.
62.		Network throughput of 320 Mbps.
63.		Should be all safety and technical regulations compliant.
64.		**PoE Switch**
65.		IEEE 802.3 Ethernet IEEE 802.3u Fast Ethernet IEEE 802.3x Flow Control IEEE 802.3af Power over Ethernet IEEE 802.3at Enhancement Power over Ethernet
66.		Hardware based 10/100/1000Mbps Auto-Negotiation and Auto MDI/MDI-X
67.		LED indicators for PoE ready and PoE activity
68.		16-Port 10/100/1000Mbps 802.3at PoE+ Ethernet Switch
69.		Switch throughput at least 30 Gbps

6.4 Door Access Control system

Sr. No.	Component	Requirement description
1.	Functionality	The system should support both biometric (fingerprint) and card reader system
2.		Should be able to configure fail – safe or fail secure mode in case of power failure of the card reader
3.		The system should include a suitable management software for configuration and operating the system.
4.		Door opening time should be configurable
5.		The card reader system must have: • Anti-pass back (APB) check facility and it must be configurable. • Facility to check the validity of the card. • Arrangement for easy installation and maintenance. • An internally rechargeable battery for storage of time settings and other settings when reader power goes off. • Self-diagnostics features for readers
6.		DC power supply inputs must be protected against over-voltage, reverse polarity and over current.
7.		Access control must read different data such as UID, Employees name, Department, Validity, D.O.B. etc. using user configured

Sr. No.	Component	Requirement description
		keysets
8.		Should be installed at all entry and exit point which includes biometric (fingerprint) & card detection for exit from the CSOC command centre and button exit configuration for rest of the site.
9.		Supports integration with UPS for uninterrupted power supply to the locks and doors.
10.		PC based software should communicate with multiple access control reader controllers using Ethernet LAN interface.
11.		Communicate with the access control readers to configure them, to fetch swipe data and to monitor their health.
12.		It should generate various reports including Access granted, Access Denied, Attempted Entry, Unused Alarm Entry, Duress Alarms log w.r.t. Date & Time
13.		Should Supports Up to 65,000 Door Controllers
14.		Compatible with all reader Hardware
15.		Time, User and Zone based Access Control
16.		Access Zones, Access Modes and Access Level configuration
17.		Access Control Features Such as 2-Person Rule, First-in User Rule, Anti-pass Back, Guard Tour, Duress Detection, Time Stamping and More
18.		Input and Output Linking
19.		Should allow editing of various access points and their interface details viz. IP address, Unit ID, Com Port.
20.		Allows editing of employee details, like name, employee number, shift, access zones.
21.		Allows modification of reader parameters, like operating mode, door open time, welcome string, Alarm settings, Timeouts, etc. These parameters are also stored in the local database
22.		Export function can be used to export data to a CSV file.
23.		Up to 10Gb data can be stored in the current tables.
24.		Older data should be moved to archives. Instantaneous Reports should be available on the current table data.
25.	Technical specification	Should be equipped with 10/100 Mbps or higher Ethernet port
26.		LED and buzzer for status, alarm, access allowed / denied
27.		Should have touch screen for fingerprint scanner
28.		Read Range maximum 3.5” for card reader
29.		Operating temperature 5 to 55 degrees or better
30.		IP65 Rating
31.		Tamper Detection
32.		Tri Color LED and Buzzer
33.		Operation mode: Network Mode with Host software
34.		Ethernet, RS-485, USB, Aux Input and Aux Output Port

6.5 Addressable fire detection and alarm system

Sr. No.	Component	Requirement description
1.	Functionality	To be installed both above and below the false ceiling
2.		Installation to be done with wall sounders
3.		System should be sheet steel painted, sealed to IP32
4.		The control panel shall be UL/FM listed The control panel shall include all required hardware, software and site specific system programming to provide a complete and operational system.

Sr. No.	Component	Requirement description
5.		A steel enclosure contains all the required components – microprocessor, power supply plus a clear LCD (Liquid Crystal Display), system status indicators and the control buttons that are the user interface.
6.		Allows the control panel to be connected to a wide variety of peripheral devices. From display repeaters to custom mimic displays, printers, serial data interfaces and switching relay interfaces.
7.		Alarm and Fault conditions are highlighted by LEDs and supported by enhanced text descriptions on the LCD display
8.		Basic functions (Evacuate, Reset, Mute, Accept, Silence) are available at one access level whilst more advanced operations are protected by a secondary level passcode
9.		Individual device isolations, test modes and configuration data are all protected by these secondary access levels
10.		Addressable Manual Call Points (Break Glass Type). The same shall be square in shape & made of ABS plastic material. Surface / Flush Mounting. It shall have a "Break glass" message embedded on the glass.
11.		Control panel the microprocessor maintains a log of the events or actions occurring on the system
12.	Technical specification	Up to 20 zone with individual LED indicators. Expandable to 40 or 80 individual LED indicators
13.		Addressable Fault / Loop isolator module with Surface mounting back box & required accessories.
14.		User controls for SOUND ALARMS, SILENCE/ RESOUND, MUTE BUZZER, ACCEPT, SYSTEM RESET
15.		Conventional Sounder / Hooter shall be made of ABS plastic material & have the Db level of minimum 85dBs and a multi tone facility, wall mounted with mounting base & required accessories / Intermittent buzzer (fault condition) High pitched continuous buzzer (fire condition)
16.		Programmable controls: Alphanumeric multi-level keypad with 15 keys and 5 control keys: YES, NO, CHANGE, ENTER and SHIFT
17.		LED type zone indicators: FIRE, FAULT/TEST/DISABLED
18.		Display: 4x40-character LCD alphanumeric display with back-light
19.		Interface: 3 serial ports with connections for optional RS485 or RS232 plug-in communication cards.
20.		Operating Temperature: 0°C to +40°C Humidity: 85% non-condensing (maximum)
21.		Loop capacity: 1 to 5 Loops expandable 460mA per loop Maximum
22.		Outputs: Sounder Outputs 2 programmable outputs. Open and short circuit monitoring. 1A maximum per output. Auxiliary Relays 1 fault and 1 fire relay voltage free, changeover outputs Contacts rated at 24V AC/DC, 1A, 0.6 PF maximum

6.6 Fire extinguisher

Sr. No.	Component	Requirement description
1.	Functionality	Device should be compliant to IS: 15683:2006 standards. Device should be stored pressure type.
2.		Should be suitable for extinguishing fires of class "A", "B" and "C".
3.		Suitable for extinguishing electrical fires.

Sr. No.	Component	Requirement description
4.		Device should be of red body color code.
5.		Device should BIS marked.
6.		Maximum weight of the filled device should not be more than 9 kilograms.
7.	Technical specification	Extinguishing media should be powder based and clean agent for DC, UPS and Hub room locations in accordance with NFPA 10-2018
8.		Expellant media should N2 based (stored pressure).
9.		Capacity of device should be minimum 4.5 kilogram.
10.		Operating temperature: -30° C to + 55° C
11.		Discharge range for extinguisher should be greater than 2 meters.
12.		Effective discharge time for the device should be 15 to 20 seconds.

6.7 Rodent repellent system

Sr. No.	Component	Requirement description
1.	Functionality	They can be installed in any sensitive area with zero risk of sparking
2.		The transducers can withstand high temperatures in the false ceilings
3.		The transducers do not need a power connection
4.		The transducers can be tested on an audible range independently, by selecting the Transducer testing menu from the LCD panel
5.		Centralised Reporting and Monitoring System. Facility to test all controllers in one go or in an individual mode
6.		Can connect up to 24 transducers with blinking LED
7.		Scheduled or Real Time health status report generation for Systems Audit
8.		Two-way Communication between the controller and the computer
9.		Support network connectivity between the transducers and the controller
10.		The OEM shall have an IDEMI and CFTRI certification for its products.
11.	Technical specification	Operating Frequency : Above 20 KHZ and below 60 KHz.
12.		Sound output: 80db to 110db at 1metre.
13.		Power output: 1W per transducer.
14.		Sweeps per Minute: 130(Configurable).
15.		Frequency Division: 100(Configurable).
16.		Power Consumption : 15 Watts Approximately
17.		Power Supply : 230V AC/ 50Hz 14 Volts DC
18.		Dimensions of panel : 225 mm X 270mm X 100mm
19.		Weight of panel : 6.5 Kgs Approx.
20.		Mounting : Wall
21.		RS / EIA 485 to RS / EIA 232C converter to transfer the controller data to the serial port of your computer
22.		LCD display with on-board controls for changing parameters

6.8 Display – for CCTV and Meeting room

Sr. No.	Component	Requirement description
1.	Functionality	The display equipment should be VESA mount ready
2.		Should have inbuilt speakers

Sr. No.	Component	Requirement description
3.		Should have colour temperature control as : Reddish, Normal, Bluish, User Mode
4.		Have a 8 bit color screen
5.	Technical specification	The display should be 32 inch diagonally.
6.		Equipped with an IPS panel with 178/178 viewing angle
7.		Having energy rating of 6.0 from Energy Star or equivalent
8.		Aspect ratio of 16:9
9.		Have maximum response time of 4 milliseconds
10.		Should have at least 1 HDMI port, 1 VGA port, 2 x USB 3.0 port, 1 DVI port.
11.		Should have at least 01 audio jack
12.		Should have minimum resolution of 1024 x 768 pixels
13.		Have refresh rate of 60 Hz.
14.		Should support video-HDMI: 480p, 576p 720p, 1080i, 1080p
15.		Should support video component:480i, 576i, 480p, 576p 720p, 1080i, 1080p

6.9 Display – Video wall with controllers and speakers

Sr. No.	Component	Requirement description
	Functionality	**Video Wall:**
1.		The Rear Projection Modules must be based on Single Chip DLP, Full HD (1920X1080) Native, Rear Projection technology. The displays shall utilize RGB Laser having different laser bank for different colors respectively without any moving part.
2.		The system should have a continuous duty cycle of 24/7 for color calibration and brightness uniformity using automated software via external server and should also support manual override function and feature on demand.
3.		No moving Part like color wheel or Phosphor wheel should be present as moving parts has more failure tendency
4.		The control of the wall shall be possible via a network. All cubes shall have their own IP address, and the control software can access all of them at the same time. The available features shall be: On/Off, Brightness and Color, Input control
5.		Separate hardware server for monitoring features Wall or Panel On/Off, Brightness and Color, Input control, health monitoring.
6.		Also, software have feature to show maximum, minimum and current brightness / color values of all the projectors.
7.		To protect operator's eyes from blue light coming from screen sitting in front of video wall can also be reduced during night time
8.		Projector should in-built green color indicator when projector is in idle state
9.		The system can also have Remote IR feature for quick basic feature without any software installation
10.		Schedule/time based ON/OFF complete system can also be possible without any human intervention
11.		Automatic / Schedule/time based backup/restore of color/brightness settings also possible
12.		Continuous consistency checking of complete system like: Duplicate IP Address, Firmware, Software Health, Cooling Load, Color & Brightness Mode, Temperature factors, etc.

Sr. No.	Component	Requirement description
13.		No single point of failure projector should be divided into multiple modules
14.		System should be green focus in the product design, 100% free of harmful substances, eco-friendly materials
		Video controller:
15.		Display Controller to be able to control mentioned video wall and should be based on the latest architecture with 19" Rack mount industrial chassis
16.		The system should have the capabilities of interacting (Monitoring & Control) with various applications on different network through the single Operator Workstation. It shall be possible to launch layouts, change layouts in real time using Tablet
17.		Keyboard and Mouse along with mechanism to extend them to 20mtrs. Operator desk from display controller to be provided
18.		The controller shall be designed for 24 x 7 operation
19.		Redundant controller should be provided
20.		The Video Wall and the Controller should be of the same make to ensure better performance and compatibility
21.		All features and functionality should be certified by the OEM.
22.		Controller cover opening alarm
23.		Resolution Support for Outputs should have 4K support
24.		Regulatory Compliance : UL, CB, BIS,FCC,CE ,IEC 60950, IEC 62368
25.		Should be possible to show Laptop Or Android / IOS phone over the video wall without disturbing the existing network over wireless
		Software:
26.		The software should be able to preconfigure various display layouts and access them at any time with a simple mouse click or schedule/timer based.
27.		The software should be able display multiple sources anywhere on video wall in any size. Key features of Video Wall management Software • Central configuration database • Browser based user interface • Auto-detection of network sources Online configuration of sources, displays and system variables
28.		Video Wall Control Software shall allow commands on wall level or cube level or a selection of cubes: • Switching the entire display wall on or off. • Setting all projection modules to a common brightness target, which can be either static (fixed) or dynamic to always achieve maximum (or minimum) common brightness between projection modules. • Fine-tune color of each cube
29.		Should support Multiple clients / Consoles to control the Wall layouts
30.		The Software should be able to share layouts b/w available different video walls on same network as well as preview of sources on the workstation
31.		Software should enable the user to display multiple sources (both local & remote) up to any size and anywhere on the display walls (both local & remote).
32.		The software should be able to create layouts and launch them as and when desired

Sr. No.	Component	Requirement description
33.		The Display Wall and sources (both local & remote) should be controlled from Remote PC through LAN without the use of KVM Hardware.
34.		Software should support display of Alarms
35.		The software should provide at least 2 layers of authentication
36.		Software should able to Save and Load desktop layouts from Local or remote machines
37.		All the Layouts can be scheduled as per user convenience. Software should support auto launch of Layouts according to specified time event by user
38.		It should be possible to schedule specific Layout based on time range It should be possible to share the layouts over LAN/WAN Network with Display in meeting room or on Remote Workstations connected on LAN/WAN Network
39.		System should have a quick monitor area to access critical functions of the video wall User should be able to add or delete critical functions from quick monitor area Full featured Web services based API supports Legacy RS-232 and TCP/IP All software communication should be encrypted, Secure user Management with AD and LDAP Support Zero Maintenance, automatically saves the user's work
40.		Integrated Embedded & External Audio formats with Audio decoding of video streams also possible Software also supports UMD, IDC, Source name, Time (time zone aware), Date, text, Logo, Message Ticker, Source Status
41.		The system shall include complete Bi-directional Soft KVM to permit operators to take mouse & keyboard control of Displays, Screen Scrapped applications and DVI source
42.		It should be possible to create two separate Tickers which run concurrently. These can be positioned at top or bottom and can run independently. The Ticker can be picked from data source through screen scrapping or through typing specific incidence, manually
43.		The system should have the capabilities of interacting (Monitoring & Control) with various applications on different network through the single Operator Workstation. It shall be possible to launch layouts, change layouts in real time using Tablet
44.		The control of the wall shall be possible via a network. All cubes shall have their own IP address, and the control software can access all of them at the same time. The available features shall be: On/Off, Brightness and Color, Input control Separate hardware server for monitoring features Wall or Panel On/Off, Brightness and Color, Input control, health monitoring.
45.		Software have feature to show maximum, minimum and current brightness / color values of all the projectors
46.		Central setup & Connection management, Central configuration database, Fully distributed & modular component technology, Browser based UI, Auto-detection of network sources
47.		Online configuration of sources, backup & restore, Scheduled backup, Fully features web services based API covering all legacy and encrypted communications
48.		Save and load layouts (complete display presets including perspectives and applications), start stop and position applications & sources freely over the complete desktop, remote keyboard and mouse control from and towards other networked desktops (bi-

Sr. No.	Component	Requirement description
		directional)
49.		Supported sources: Analog & digital / streaming video, Analog (RGB) and Digital (DVI-I) Sources, Network desktops, Network multi-channel workstations and applications, Internet & internet sources, Embedded & external audio formats, Localization
50.		**Speaker:**
51.		Should be a sound bar to be installed with the video wall connected to the video controller.
52.		Should support surround sound audio output with additional wired woofer.
53.		Should be compatible with both the display and the controller.
54.		Should support Bluetooth feature.
	Technical specification	**Video Wall:**
55.		All cubes shall of 70" diagonal size and optimized to work in a multi-screen arrangement (4 X 2)
56.		> 700 Nits on screen
57.		Laser with lifetime minimum 100000 hours
58.		Panel uniformity should be >95%
59.		Color repetition speed must be 18X Frame Rate or higher with 3 x 12-bit color and Brightness correction
60.		Projector is equipped with Automatic motorized alignment no manual alignment needed
61.		Redundant Power Supply External remote one to be provided only This should be kept in the rack so that power supply can be changed without disturbing any cube or alignment.
62.		Should be IP6X certified by third party laboratory
63.		Projector should complies with EMC (Electro-Magnetic Compatibility) Standard
64.		Each display module shall have minimum Redundant DP1.2 and HDMI 1.4 (HDCP compliant), DVI-DL inputs for redundancy purposes
65.		Projector should capable of gen-lock 49 Hz - 61 Hz; 92 -120 Hz, also supports double genlock
66.		Serviceability should be rear
67.		Native Resolution per Panel should be minimum 1920x1080
68.		Aspect Ratio should be 16:09
69.		Screen Gap should be Less Than 1mm
70.		Contrast ratio should be Min 1800 Lumens
71.		Power consumption should be Less than 200 watt in Normal/Typical Mode
72.		Heat Dissipation should be Less than 800 BTU/hr.
73.		System shall operate properly under 10ºC to 40ºC Temperature , Humidity - 20%-80%
74.		All features and functionality should be certified by the OEM.
		Video controller:
75.		Operating System : Windows 10 or higher , 64-bit
76.		Xeon with 2.1 GHz or higher end processor, Octa core
77.		Memory minimum 32 GB expandable to 64 GB
78.		2 x 1Gb/s / 10 Gb/s LAN
79.		Input : H.264, MPEG2/4, MxPEG, MJPEG, V2D, H.263
80.		Output : DP/DVI/HDMI, Outputs - Up to 48 HD displays
81.		Hard Disk - R.A.I.D-1 redundant setup with 2x 1000GB 2.5" HDD

Sr. No.	Component	Requirement description
		Hard disk
82.		4ch Graphic card , Max resolution: 3840x2160@60Hz
83.		**Speaker:**
84.		Sound bar should be of 2.1 channel with wired sub-woofer.
85.		Should support audio connectivity through HDMI port, Bluetooth, wireless connectivity, auxiliary, etc.
86.		Should have maximum wattage of 110W.
87.		Should be equipped with power adapter and audio cables.
88.		Any additional items should be proposed by bidder with cost inclusive.

Note: Any accessories or hardware required for the solution should be proposed by the bidder with cost included in the solution. The bidder has to specify what additional hardware / accessories has been proposed.

6.10 Network Rack

Sr. No.	Component	Requirement description
1.	Functionality	Type of rack should be rack enclosure.
2.		Rack should be free standing type.
3.		The front door of the rack should be of toughened transparent glass.
4.		The rear door of the rack should be of SPCC quality cold rolled steel metal.
5.		Back doors should be perforated with 63% or higher perforations
6.		Should be available with secure lock
7.		Should be equipped with cable channel in the rear side for cable management
8.		Should support entry of cable from top or bottom of the rack
9.	Technical specification	Size of rack should be 42U
10.		Depth of the rack should be 1000 millimeter (adjustable)
11.		Width of rack should be 600 millimeter
12.		The front and rear doors should open a minimum of 120 degrees to allow easy access to the interior
13.		Should have a load bearing capacity of minimum 1200 kilograms
14.		Should have at least one fan for heat dissipation
15.		Should be RoHS compliant
16.		Should be UL Listed and conform to EIA-310 Standard or India equivalent for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard x
17.		Should have a minimum of IP 20 rating for protection against touch, ingress of foreign bodies, and ingress of water
18.		Should be equipped with at least two power strips or PDU.

7. Minimum technical requirement (IT assets)

7.1 Security Orchestration Automation & Response (SOAR)

Sr. No.	Component	Requirement description
1.	Functionality	SOAR solution should be flexible enough to allow security operations to easily create bidirectional integrations with security products not supported by default.
2.		The methods used to support these types of integrations could vary but might include scripting languages, APIs or proprietary methods.
3.		SOAR platform should support common methods of data ingestion, such as syslog, database connections, APIs, email and online forms, as well as common data standards such as CEF, Open IOC, STIX/TAXII, etc.
4.		SOAR solution should have ability to automate and orchestrate process workflows to achieve force multiplication, and reduce the burden of repetitive tasks on security analysts.
5.		SOAR solution should support flexible methods for implementing process workflows.
6.		Should be able to automatically extract email attachments from emails and store that for the related incidents as attachments.
7.		Solution should include 100+ out-of-the-box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DOS and DDOS attack, Phishing Attack, etc. and should support creation of multiple playbook.
8.		Solution must be able to support creation of incidents via API, Web URL, SIEM, Ticketing system, etc.
9.		Should support codify process like linear-style playbooks, flow-controlled workflows or run books.
10.		Should have out-of-the-box provision or capable of creation and closure of incident automatically or manually.
11.		Should have capability to execute automated workflow without any human intervention.
12.		Should have capability to provide simulation environment to test playbooks without relying on access to real environment.
13.		Should provide option in workflows for manual intervention/review/approval by analyst to choose decision path before playbook can continue or to complete a task manually before playbook can continue.
14.		Implementation of workflows should be flexible enough to support nearly any process which might need to be codified within the solution.
15.		Workflows should support the use of both built-in and custom integrations, as well as the creation of manual tasks to be completed by an analyst.
16.		Should have the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system.
17.		Flow controlled workflows should be able to support different types of flow control mechanisms, including those which allow for an analyst to make a decision manually before the workflow continues.
18.		Building workflows should not require a high level of scripting or programming knowledge and should be based on a GUI platform.
19.		The solution should support basic case management functionality

Sr. No.	Component	Requirement description
		such as tracking cases, recording actions taken during the incident and reporting on critical metrics and KPIs.
20.		The following additional features should be available in the SOAR solution: • Phase and objective tracking • Detailed task tracking, including assignment, time spent and status • Asset management, tracking all physical and virtual assets involved in the incident • Evidence and chain of custody management • Indicator and sample tracking, correlation and sharing • Document and report management
21.		Auto-document the entire incident workflow manual as well automated steps for all incidents timestamp of all actions taken in an incident.
22.		Provide automated report & dashboards for real time measurement of KPI's including MTTD, MTTR for each incident and overall SOC incidents.
23.		Provide automated incident SLA breach report based on severity, type, creation time, closure time, response time etc.
24.		Should develop reports by tracking of indicators and samples, such as IP addresses, URLs, malware samples, etc.
25.		Should have threat intelligence feeds to properly correlate to the end of discovering attack patterns, potential vulnerabilities and other ongoing risks to the organization.
26.		Should the capability for different forms of threat hunting, while actively looking for attacks and patterns that may not have been detected through automated methods.
27.		Should be able to integrate with all devices irrespective of the OEM or manufacturer.
28.		Should be able to provide insights like status, incidents, detections, etc. for different devices on a single platform. User should be able to access all information without logging out of the SOAR solution.
29.		Should support email or text notifications, along with functionality to email comprehensive periodic reports and dashboards.
30.		Solution should support the ability to correlate against third party security data feeds.
31.		Solution be agentless and should support both push and pull mechanism.
32.		Should be able to parse all the fields from SIEM, UEBA, NTA alerts including but not limited to: creation time, update time, source / destination IP, source country, category, system, rule-name, severity, etc.
33.	Technical requirement	Should support at least four analysts' user accounts and support scalability for increase in the number of analyst accounts.
34.		Should support a web-based GUI for management, analysis and reporting.
35.		Should support recreation of any incident for simulation and analysis purpose.
36.		Should be able to locally store evidence for each alert/incident raised by it along with capability to search through it.
37.		Should have intuitive, modular, analyst friendly user interface for overall incident management and interface to add/ edit response tools.

Sr. No.	Component	Requirement description
38.		Solution should not have any restriction on the number of response actions and creation of playbooks.
39.		Should provide capability to embed scripts (Python / java / JS or any other language code) in the playbooks steps to design playbooks for advance and complex use cases.
40.		Should be able to auto-document the entire incident workflow manual as well automated steps for all incidents timestamp of all actions taken in an incident.
41.		Solution should have capability to design workflow to provide fully automated action for any incident.
42.		Solution should have provision for storing security incidents/alerts and related artefacts for minimum 1 year. Data retention & data archival settings should be or configurable as per the decision of OCAC.
43.		Should have at least 150 out of the box API based integrations and additional integrations should be free.
44.		Should be able to integrate existing SIEM /ESM solution irrespective of the OEM and version.

7.2 Log Management appliance

The log management appliance should be capable and compatible to integrate with the below devices:

1. Security Information and Event Management / ESM
    a. Make: HPE ArcSight
    b. Appliance Model: ESM E7600
    c. EPS Support: 10000 EPS
    d. Operating System: RedHat Enterprise 7.1 (Maipo)
2. Logger device
    a. Make: HPE ArcSight
    b. Appliance model: L7600 / product version L7633
    c. Operating system: RedHat Enterprise
    d. License type: Permanent
    e. Software version: 6.7 or higher
3. Connector device
    a. Make: HPE ArcSight
    b. Appliance model: C6600
    c. Operating System: RedHat Enterprise
    d. License type: Permanent
    e. Software version: 2.9 or higher

Note:

1. The bidder shall be responsible for the integration of the above mentioned solutions with SOC.
2. The bidder is provided with an option to either upgrade the existing solutions & utilize for SOC or may propose a new SIEM solution along with logger appliances, however the existing solution shall be integrated with SOC.
3. The bidder may follow as prescribed in Section 3.5: "General Instructions to bidders" of the RFP document.

Sr. No.	Component	Requirement description
	Functionality	**Logger**
1.		Should function in Client server model.
2.		Should support collection of logs from all devices irrespective of manufacturer and version.
3.		Should have filtering, parsing, rewriting, normalization functionality.
4.		Should be able to make rapid searches though billions of messages.
5.		Should be capable of complex searches and drill down results.
6.		Should be capable to generate alerts based on automated queries.
7.		Should easily be able to integrate with other third party tools and solutions.
8.		Should be able to integrate with existing SIEM or SOAR solution.
9.		Should support agent and agent-less detection and collection of logs from devices.
10.		Create customized reports to demonstrate compliance with standards and regulations such as PCI-DSS, ISO 27001, ETC.
11.		Classify incoming logs in real-time based on message content, extract named information elements from unstructured log messages, allowing you to aggregate disparate log formats to search and generate statistics.
12.		Solution must support the option of collecting raw event data using Syslog, FTP,SCP, SNMP protocols, and any other protocol required for collection of logs etc.
13.		Parsing and rewriting capabilities to transform and normalize to enable effective search and analysis.
14.		Solution must provide a native, out of the box capability to collect application log data from custom /in-house developed web applications or bidder may develop custom parser to ingest custom logs.
15.		Should have automatic data archiving feature.
16.		The solution should prevent tampering of any type of logs and log any attempts to tamper logs.
17.		Store log data in encrypted, compressed, and timestamped binary files, restricting access to authorized personnel only
18.		Index logs that enable organizations to segment their log data based on any number of criteria and restrict access to logs based on user profiles.
19.		Should be able to Integrate with the existing SIEM solution irrespective of the OEM and version.
20.		Solution should have capacity to maintain and store logs (raw and normalized) for minimum 90 days online.
21.		Should integrate with SAN storage for offline storage of logs.
22.		Solution must be able to store log data both locally and with SAN integration.
23.		Solution must provide inline options to reduce event data at the source by filtering out unnecessary event data.
24.		Management should be available through Web browser, CLI, Web services API.
		Connector
25.		Should offer ease of analysis through a common event format for all log sources.
26.		Should provide complete visibility with collection support for any event source from the physical layer through the application layer.

Sr. No.	Component	Requirement description
27.		Management should be available through Web browser, CLI, Web services API.
28.		Should support universal content relevance with prebuilt, vendor-independent content.
29.		Should not have restriction in the number of devices to be integrated.
30.		Solution must support the option of collecting raw event data using Syslog, FTP,SCP, SNMP protocols, and any other protocol required for collection of logs etc.
31.		Solution must support local caching and batching at collection level in case of connectivity failures.
32.		Solution should work in both agent-less and agent-based mode.
33.		In case the connectivity with SIEM / logger management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.
	Technical specification	**Logger**
34.		Should have hot swappable dual power supply.
35.		Forward logs to 3rd party analysis tools or fetch data from SSB via its REST API.
36.		Licensing for at least 20000 EPS and expandable whenever required.
		Connector
37.		Should have hot swappable dual power supply.
38.		Should support handling and processing of least 20000 EPS and expandable whenever required.

7.3 Security Information and Event Management (SIEM)

Sr. No.	Component	Requirement description
1.	Functionality	The OEM of the solution should be in the Gartner, Forrester, IDC, NSS, etc. leader quadrant in any of the last three years.
2.		Solution should encompass log, packet and end point data with added context and threat Intelligence.
3.		The solution should factor with following minimum components: · Management & Reporting · Normalization and Indexing · Correlation Engine · Data Management
4.		There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department. The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required
5.		The solution should provide an integrated dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role based access control mechanism and handle the entire security incident lifecycle.

Sr. No.	Component	Requirement description
6.		Solution should categorize log data into an easy-to-understand humanly-readable format that does not require knowledge of OEM-specific event IDs to conduct investigation, define new correlation rules, and/or create new reports/dashboards.
7.		All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement; normalization should be performed to meet the reporting and analysis needs.
8.		Should be manageable and monitored from SIEM unified GUI console for Correlation, Alerting and Administration.
9.		Solution search performance must be capable of searching through millions of structured (indexed) and unstructured (raw log) events.
10.		Should assist analysts by reducing false positives automatically without configuring any rules or filters to do so.
11.		SIEM solution should be able to consume the Threat Intelligence Feed as proposed in the solution.
12.		Seamless and bidirectional integration with SOAR and Vulnerability Management platform for incident workflow management.
13.		SIEM solution should provide a centralized customizable dashboard as required in SOC functionality.
14.		Must be able to integrate and work with the current systems of the organization and its stakeholders.
15.		Solution should help in creating the context around the Vulnerability by integrating proposed vulnerability management solution which can further create the priority as per asset & vulnerability record.
16.		Solution should not require a Database Administrator to perform implementation, tuning or other DB administrative tasks.
17.		Solution should have Self-signed certificate generation features so that access of appliance for monitoring and administration purposes can be done in encrypted manner.
18.		Solution must provide a web interface for mapping to remote file systems using NFS or CIFS to backup log data or read raw log files into the system.
19.		Solution must provide pre-defined alerts and provide the ability to reuse pre-defined filters and manually created filters as alert criteria.
20.		The solution should support a. Monitoring and notification of events; b. Incident Handling and Investigation support; c. Import of vulnerability scanning information; d. Analysis and report; e. Operation management of SOC
21.		Should be able to handle and process complete EPS as forwarded by the logger devices and scalable for upgradation for future requirement.
22.		Solution must provide inline options to reduce event data at the source by filtering out unnecessary event data.
23.		It should be able to handle a burst of 1.25 times of the sustained EPS in real time at any given point in time without any drop or queuing of events.
24.		Should be able to integrate with the existing SIEM solution and proposed SOAR solution.

Sr. No.	Component	Requirement description
25.		Integration should be bi-directional with the SOAR solution.
26.		Solution should log all administrative access and activities and provide access to the audit logs web interface.
27.		Should support storage and archiving of data and reports as per requirement.
28.		Solution should be able to restore from archives / external storage and generate reports whenever required.

7.4 Anti – Advanced Threat Persistent (Anti – APT)

Sr. No.	Component	Requirement description
1.	Functionality	The OEM of the solution should be in the Gartner, Forrester, IDC, NSS, etc. leader quadrant in the latest reports.
2.		Lock down patient zero, stop the spread, and neutralize the attack at the initial point of infection before it spreads laterally.
3.		Solution must be on premise Anti-APT solution and must not be network perimeter security component part devices like UTM and NGFW and not be a CPU and chip based function.
4.		Increased protection against advanced persistent threats with static and dynamic detection techniques
5.		Enhance security intelligence similar to NGFW and NGIPS "learn" from attacks.
6.		Solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list.
7.		Use specialized detection engines, correlations rules, and custom sandboxing to detect all aspects of an advanced persistent threat, not just malware.
8.		Should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attacks sessions.
9.		Should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a dashboard
10.		Leverage detection data to create new rules and policies to block existing and future attacks.
11.		The solution should be OS agnostic and should deploy static/dynamic analysis for emulation of threats on various operating systems like Windows, MAC, Linux, etc. irrespective of the versions. The solution should support Windows 7, Windows 8, Windows 10 Microsoft 2003, Microsoft 2008, Microsoft 2012, and Microsoft 2016 operating environments for Sandboxing, this requirement should be based on virtual execution and should not be Hardware or chip based function.
12.		Capable of monitoring all ports and protocols to identify attacks anywhere on the network.
13.		Capable of examining email attachments using multiple detection engines and sandboxing. Prevent new and unknown attacks in documents and executable files
14.		Attachments analysed should include a wide range of Windows executables, Microsoft Office, PDF, Zip, Web content, and compressed file types. Identify new malware hidden in files types, including but not limited to: Adobe PDF, Microsoft Office, Java, Flash, executables, and archives
15.		Malware protection should be done by specialized detection and

Sr. No.	Component	Requirement description
		sandboxing techniques, which can discover malware and exploits delivered in common office documents.
16.		Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp and solution should have an in-built document vulnerabilities detection engine to assure analysis precision and analysis efficiency.
17.		Capable of analyzing URLs contained in emails using reputation, content analysis, and sandbox simulation.
18.		Capable of unlocking of password-protected files and Zip files
19.		Capable of combining global telemetry from one of the world's largest cyber intelligence networks, with local customer context, to uncover attacks that would otherwise evade detection
20.		Supports SPAN port or port mirroring configuration
21.		Able to integrate with multiple devices and analyze all information in parallel
22.		Able to protect from both known and unknown threats utilizing IPS, Antivirus, Anti-Bot, Threat Emulation (sandboxing) and malicious content detection and real-time elimination technologies.
23.		Able to monitor the instruction flow at the CPU-level to detect exploits attempting to bypass OS security controls
24.		Capable of decrypting protected SSL and TLS tunnels to extract and launch files to discover hidden threats.
25.		Prevents and remediates evasive ransomware attacks
26.		Blocks deceptive phishing sites and alerts on password reuse
27.		Protects applications against exploit based attacks
28.		Records and analyzes all endpoint events to provide actionable attack forensics reports
29.		The solution should be able to inspect and block all network sessions regardless of protocols for suspicious activities or files at various entry/exit sources to the client's network.
30.		The solution should be able to protect against Advanced Malware, zero day web exploits and targeted threats without relying on signature database.
31.		The solution should be able to identify malware present in network file shares and web objects (QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, ico, jar, jpeg, jpg, mov.) and able to quarantine them.
32.		The solution filter must support network action set such as Block (drop packet), Block, Permit, Trust, Notify, Trace, Rate Limit and Quarantine & must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic
33.		The solution should be able to identify zero-day malware present in file and web objects (Adobe Flash File, Java, Microsoft Office Files .doc .docx .ppt .pptx .xls .xlsx, .pdf, rar, dll, sys, tar, exe, zip, bzip, 7zip, ink, chm, swf etc.) and should have ability to interrupt malicious communication.
34.		The proposed solution should support at least 100+ protocols (e.g. HTTP, FTP, SMTP, SNMP, IM, IRC, DNS and P2P protocols SMB, Database protocol MySQL, MSSQL, Microsoft Office, Visual Basic, Acrobat PDF, MAC OS X *.app, zip, tar, flash, executables, link libraries, etc.) for inspection and should block suspicious

Sr. No.	Component	Requirement description
		communications of zero day malware detected IP, URL and file.
35.		Solution should identify spear fishing email, zero day malware and ransomware attacks in email and should quarantine or block suspicious email messages before reaching user/ mail server.
36.		The solution should support Sandbox test environment which can analyse threats to various operating systems, browsers, databases etc.
37.		The solution should support both inline and out of the band mode.
38.		The solution should be able to detect and prevent bot outbreaks including identification of infected machines.
39.		The solution should be appliance based with hardened OS. No information should be sent to third party systems for analysis of malware automatically.
40.		The solution should be able to block the call back tunnel including fast flux connections.
41.		The solution should be able to share malware information/ zero day attacks knowledge base with deployed appliances.
42.		The solution should be able to capture packets for deep dive analysis.
43.		In case there is no antivirus signature available for malware, solution should have the ability to exfiltrate data about the malware and share it with the antivirus solution providers.
44.		The solution should be able to pinpoint the origin of attack, Threat description and help to understand the severity and stage of each attack.
45.		The solution should be able to conduct forensic analysis on historical data.
46.		Dashboard should have the feature to report Malware type, file type, CVE ID, Severity level, time of attack, source and target IPs, IP protocol, Attacked ports, Source hosts etc.
47.		The solution should generate periodic reports on attacked ports, malware types, types of vulnerabilities exploited etc.
48.		The solution should be able to export event data to existing SIEM or Incident Management Systems.
49.		Solution should be able to monitor encrypted traffic.
50.		The management console should be able to provide information about the health of the appliance such as CPU usage, traffic flow etc.
51.		The solution should display the geo-location of the remote command and control server.
52.		The solution should be able to integrate with Active Directory to enforce user based policies.
53.		The solution should monitor Inter-VM traffic on a Port Mirror Session.
54.		Sandboxes must support multiple operating systems and for both 32-bits and 64-bits OS.
55.		The solution should support Windows XP, Windows 7, Windows 8, Windows 10 Microsoft 2003, Microsoft 2008, Solaris10, Redhat 5 & above Linux operating environments for Sandboxing, this requirement should be based on virtual execution and should not be Hardware or chip based function.
56.		The solution should support open web Services API for 3rd party or scripting integration.
57.		Solution should allow admin to define custom threat intelligence by importing/exporting rules.
58.		The solution should support windows XP, Windows 7, Windows 8, windows 10 Microsoft 2003, Microsoft 2008 (32 bit & 64 bit OS),

Sr. No.	Component	Requirement description
		Solaris10, and RedHat 5 & above Linux operating environments for Sandbox file analysis. Solution should have option to upload custom sandbox image running in client's environment.
59.	Technical specification	Minimum performance throughput up to 2 Gbps
60.		Should be able to store online data for at least 90 days.
61.		Capable of performing multiple sandboxing environment in parallel, handling more than 50 virtual machines
62.		Capable of processing more than 4000 unique files per hour and have provision for expansion whenever required
63.		Supports OS: Win 10 (64-bit), Win 8.1 (64-bit), Win 8 (32-bit/64-bit), Win 7 (32-bit/64-bit), Win XP (32-bit/64-bit), Win Server 2016, Win Server 2012, Win Server 2012 R2, Win Server 2008, Win Server 2003, Android, Mac, Linux
64.		Capable of generating reports in the following formats: STIX, OpenIOC, XML, JSON, HTML, PDF, text
65.		Capable for in-line, TAP / SPAN, monitoring and Fail-open operation
66.		Should be capable to add multiple number of monitoring nodes logically.
67.		Should support scalability in number of ports for expansion.
68.		Hot swappable dual power supply
69.		Have maximum MTBF and least MTTR

7.5 Network Traffic Analyzer

Sr. No.	Component	Requirement description
1.	Functionality	Identify what applications/protocols are running on the network.
2.		Identify bandwidth hogs down to a user, application or device level.
3.		Monitor client to server network traffic.
4.		Troubleshoot network & application performance issues.
5.		Should be pre-built with hundreds of reports, graphs, and charts, which are all customizable.
6.		Bandwidth Utilization and flow / packet based Monitoring and reporting
7.		Should be able to monitor from L2 to L7 layer metrics conversations in the network.
8.		Should support deployment of multiple sensors/probes to acquire data from multiple sources in the network, multiple systems/appliances running analytics engine components for better assessment of traffic to security profiles, multiple systems/appliances with deep-learning/machine-learning components for anomaly detection and, multiple systems/appliances with web-UI components supporting high-availability and scalability needs.
9.		Spot users or devices downloading large volumes of data.
10.		Bandwidth Usage by Application
11.		Should support use of aggregation policies (sum, average, minimum, maximum, etc.) that work on volumetric data counters such as bytes, packets, non-empty packets, etc.
12.		Should support use of policies that can detect spikes of quantum (1x, 2x or a user-configurable jump or fall) in network traffic.
13.		Should be to spot top talkers on the network.
14.		Should be able to auto discover assets communicating in the network.

Sr. No.	Component	Requirement description
15.		Should have deep-learning/machine-learning component to detect anomalous and suspicious communication is network traffic irrespective of its origins or destination and, protocol or application.
16.		Should support use of policies that can detect violations based on blacklist/whitelist matches.
17.		Should have basic monitoring statistics like tracking source IP, destination IP, protocols and bandwidth.
18.		Should be capable of bulk decryption of SSH, IPSec, HTTPS, SMTPS, IMAPS, SSL, TLS, etc. encrypted traffic for analysis and monitoring.
19.		Should integrate with SOAR or log management tools for sharing of network data in real time and, alerts as they happen.
20.		Should include a distributed search engine data-store to ingest various types of textual, numerical, geospatial, structured and unstructured data.
21.		Should allow for proactive investigation by allowing user to interact with data using visual graphs/charts in interactive dashboards.
22.		Should enable user to investigate network performance or security issues by accessing details about session. The details may pertain to delays, gaps, session initialization or termination reasons, session payload and data enrichments.
23.		Should be able to generate and retrieve reports for a minimum of one year period where online data should be available for minimum 90 days period.
24.		Should consist of a sensor or probe to acquire network traffic or flow data and generate session metadata from the acquired traffic.
25.		Should include an analytics engine component that processes network traffic and/or generated session metadata to detect threats, risks and, anomalies.
26.		Should support for reconstruction of session if raw capture retention is configured.
27.		Should not require an internet connection in support of any of its capabilities. It should be possible to schedule ingestion of OEM supplied and third-party threat intelligence by importing the update using system console or CLI or scheduling checks with a locally hosted repository.
28.		Should support anomaly detection without any threat intelligence in place by using its deep-learning/machine-learning capabilities.
29.	Technical specification	Should support minimum 10 Gbps of throughput performance.
30.		Should support SPAN / port mirroring.
31.		Should support monitoring unlimited number of nodes logically.
32.		Should support scalability in number of ports for expansion.
33.		Should support minimum 5,00,000 HTTP transactions.
34.		Operating system should be security hardened and embedded with overlaying kernel for high speed packet processing.
35.		Appliance should have hot swappable dual power supply.
36.		Should be licensed to monitor traffic from unlimited number of nodes.
37.		Protocols like HTTP, SMB, RDP, SSL, DNS, SMTP, LDAP, etc. should be detected by the solution.
38.		Should support any web browser for management or monitoring through a workstation.
39.		Monitor network traffic through SNMP, Netflow, WMI, Rest APIs, etc. and network sniffing.
40.		Should be able to generate and retrieve reports within the appliance

Sr. No.	Component	Requirement description
		itself without the use of any additional database server.
41.		Should be able to integrate with external storage devices for storing and retrieving if old records / data.

7.6 Threat Intelligence feeds

Sr. No.	Component	Requirement description
1.	Functionality	Intelligence feeds should be available from open sources, commercial sources and international sources.
2.		Threat Intelligence should deliver a comprehensive range of timely adversary and technical threat intelligence through a customizable portal or Dashboard.
3.		The Threat Intelligence Portal/Dashboard should provide a complete range of adversary and technical intelligence.
4.		The Threat Intelligence Portal/Dashboard should provide End-to-End picture of threats.
5.		Intelligence feeds should adhere to MITRE and ATT&CK framework.
6.		Threat Intelligence feeds should contain who, how and why are you being targeted.
7.		Intelligence feeds should be integrated with SOAR / SIEM solution and should be pushed towards the respective devices for upgradation.
8.		Threat intelligence feeds should enable efficient security operations and reduce the time for investigation.
9.		The intelligence feeds should be available for the complete proposed solution and pushed periodically.
10.		Intelligence feeds from all sources should be provided as a bundled single input.
11.		Should have inputs preferable from dark web and similar kind of sources.
12.		The threat intelligence feeds should be available in multiple formats.
13.		Intelligence feeds should be reliable to eliminate maximum number of false positives and reduce duplicity in threat definitions.
14.		Should provide advanced IP Reputation.
15.		Should provide the data feed in formats intercept able by the SOC solutions
16.		Provide scripts based feeds whenever required to download the data feeds.
17.		Should provide additional information in IOCs wherever requested.
18.		Threat Intelligence feed OEM should have experience of at least 10 years.
19.		Threat Intelligence feed has to be unique. This has to be from a different OEM and not the same as of SIEM / SOAR OEM to adhere to the dual incident monitoring design principle.
20.		Threat intelligence should provide an insight into current and emerging threats.
21.		Intelligence feeds should cater to all SOC solutions and equipment.
22.		Intelligence feeds should also preferably include feeds from the OEM providing the security hardware in-order to provide an integrated cyber-defense and data exchange between devices.

7.7 Network Management Switch for Data centre

Sr. No.	Component	Requirement description
1.	Functionality	Layer 3 access switch to be installed at data centre.
2.		Should be rack mountable and easily installable.
3.		Should have in built redundant, hot swappable power supply.
4.		Should have internal redundant cooling fan.
5.		Should have a console port.
6.		Should be IPV4 and IPV6 ready from day one.
7.		Supports Layer 2 protocols: 802.1Q VLAN, 802.3xVLAN.
8.		Supports Layer 2 protocols: LACP, STP, MSTP, RSTP.
9.		Supports Layer 2 protocols: VxLAN, IEEE.
10.		Supports Layer 3 protocols: Static routing, RIPv1, RIPv2.
11.		Supports Layer 3 protocols: BGP, OSPFv2, OSPFv3, RIPng, PBR, BGP4.
12.		Supports Layer 3 protocols: PIM-SM & SSM & DM, IS-IS, IS-ISv6.
13.		Supports Layer 3 protocols: VXLAN, VRRP, DCBX.
14.		Supports Layer 3 protocols: 802,1Qbb, 802,1Qaz, FCoE, etc.
15.		Should be equipped with security feature: Snooping, dynamic ARP, ACL, RADIUS / TACAS, Port security, IGMP snooping, DHCP, etc.
16.		Support management protocols: GUI / GUI using NMS
17.		Support management protocols: CLI, Telnet, TFTP
18.		Support management protocols: SNMPv1, SNMPv2, SNMPv3
19.		Support management protocols: NTP, SSHv2, DLDP/UDLD
20.		Support management protocols: Hitless patch upgrades, IP management, Openflow, etc.
21.		Should support: LDP protocol, MCE, P/PE of MPLS VPN, MPLS Traffic Engineering (TE), MPLS Operations, Administration, and Maintenance
22.		Should be RoHS compliant.
23.	Technical specification	Should have minimum 24 x 10GE SFP+ ports.
24.		Should at least one management port of GE management interface, RJ45 and optional management port of RS232 / USB.
25.		Should have minimum switching capacity of 450 Gbps.
26.		Should have minimum MAC address table size of 128K
27.		Should be capable of configuring more than 500 IPV4 and 5000 IPV6 routing.
28.		Should have in built, preinstalled operating system.
29.		Should support minimum 4000 VLAN and VLAN IDs.

7.8 Network Router for SOC Command Centre

Sr. No.	Component	Requirement description
1.	Functionality	LED indicators for Ethernet and console status, as well as visual system state indications
2.		Command-line interface (CLI), alarm, network management, logging, statistics aggregation, and on-board failure logging (OBFL).

Sr. No.	Component	Requirement description
3.		Environmental chassis management
4.		Minimum 20 Gbps sustained forwarding data traffic capacity
5.		One Network Interface Module (NIM) bay.
6.		Dual In-line Memory Modules (DIMMs)
7.		USB flash or secure token memory stick
8.		Should have dual power supply
9.		Should support IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2)
10.		Should support Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector,
11.		Should support Multicast Internet Group Management Protocol Version 3 (IGMPv3
12.		Should support Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), RSVP, CDP, ERSPAN, IPSLA, Call Home, EEM, IKE, ACL, EVC, DHCP, FR, DNS, LISP, OTV[6], HSRP, RADIUS, AAA, AVC, Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast
13.		Should support MPLS, Layer 2 and Layer 3 VPN, IP sec, Layer 2 Tunnelling Protocol Version 3 (L2TPv3)
14.		Should support Bidirectional Forwarding Detection (BFD), IEEE802.1ag, and IEEE802.3ah
15.		Should support Generic routing encapsulation (GRE)
16.		Should support Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP)
17.		Should support Frame Relay, Multilink Frame Relay (MLFR), High-Level Data Link Control (HDLC)
18.		Should support Serial (RS-232, RS-449, X.21, V.35, and EIA-530)
19.		Should support PPP over Ethernet (PPPoE)
20.		Should support QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED)
21.		Should support Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing and NBAR.
22.		Should support Encryption: DES, 3DES, AES-128 or AES-256 (in CBC and GCM modes)
23.		Should support Authentication: RSA (748/1024/2048 bit), ECDSA (256/384 bit)
24.		Should support Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512
25.		Features such as quality of service (QoS), cryptography, and access control lists (ACLs) are processed in hardware.
26.		Modular QoS CLI (MQC) policies on VLANs or tunnels
27.		Limits an arbitrary collection of low-priority traffic to a certain bandwidth
28.	Technical specification	RJ-45 console ports and auxiliary ports, and a mini USB console port.
29.		One copper Ethernet 10/100/1000 Mbps network management port.
30.		Two USB 2.0 ports for USB flash sticks or USB secure tokens (secure key distribution).
31.		Minimum aggregated throughput of 01 Gbps from Day 01
32.		Minimum 4 x 1 GE Base-T interfaces
33.		Minimum 4 x 10 GE SFP+ interfaces

Sr. No.	Component	Requirement description
34.		One RJ-45/RS-232 compatible auxiliary port

7.9 Managed Switch for SOC Command centre

Sr. No.	Component	Requirement description
1.	Functionality	Should be of Non-PoE type with form factor of 1U.
2.		Should be rack mountable and easily installable.
3.		Should have internal redundant cooling fan.
4.		Should have a console port.
5.		Should be IPV4 and IPV6 ready from day one.
6.		Should support Layer 2 features: IEEE 802.1Q tagged VLAN
7.		Should support Layer 2 features: IEEE 802.1D Spanning Tree Protocol
8.		Should support Layer 2 features: IEEE 802.1D Spanning Tree Protocol
9.		Should support Layer 2 features: IEEE 802.1v Protocol VLAN & Port VLAN and MAC-based VLAN, Voice VLAN, Guest VLAN, IP subnet-based VLAN
10.		Should support Layer 2 features: IEEE 802.1 Q-in-Q – IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree, IEEE 802.3ad Link Aggregation (LACP), IEEE 802.1x port access authentication
11.		Should support Layer 2 features: IGMP v1, v2, v3 snooping support, IGMP querier
12.		Should support Layer 2 features: Static multicast filtering, Weighted round robin (WRR) queue technology, MLD v1, v2 snooping
13.		Should support Layer 3 features: Static routing, ARP
14.		Should support security features: Access Control Lists (ACL), MAC, IP, TCP, ACLs: L2/L3/L4
15.		Should support security features: Network storm protection including broadcast multicast and unicast traffic
16.		Should support security features: Protected ports, MAC filtering, Private group
17.		Should support security features: IEEE 802.1x port access authentication, Port security
18.		Should support security features: DoS, DHCP snooping
19.		Should support security features: IP Source Guar, Dynamic ARP inspection
20.		Should support security features: RADIUS (RFC 2865), RADIUS accounting (RFC 2866), TACACS+
21.		Should support switch management features: SNMP v1, v2c, v3 with multiple IP addresses
22.		Should support switch management features: Private Enterprise MIB, Port mirroring support (many-to-one)
23.		Should support switch management features: DHCP/BOOTP relay-

Sr. No.	Component	Requirement description
		primary and backup (RFC 3046, option 82), RFC 2030 Simple Network Time Protocol (SNTP), DHCP server, DHCP L2 relay
24.		Should support switch management features: IEEE 802.1AB Link Layer Discovery Protocol (LLDP), ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED), DHCP relay (with backup servers), GARP/GVRP/GMRP
25.		Should support switch management features: SYSLOG, TFTP, SFTP, HTTP, SCP, or local USB flash firmware upgrade
26.		Should support switch management features: Port description – RFC 1519 CIDR
27.		Should support switch management features: Proxy ARP, DNS lookup
28.		Should support user interfaces: Command Line Interface (CLI) via console port (5 sessions), Web-based management via embedded HTTP server protected with Secure Sockets Layer, (SSLv3) or Transport Layer Security (TLS v1), Telnet remote login (5 sessions) securable with Secure Shell (SSH v1.5, v2)
29.		Should have preinstalled operating system.
30.	Technical specification	Should have minimum 48 x 10/100 Base TX ports and 4 x 100/1000 SFP/SFP+ ports.
31.		Should at least one management port of RJ45 and another management port of RS232 / USB.
32.		Should have minimum switching capacity of 15 Gbps.

7.10 SAN Storage

Sr. No.	Component	Requirement description
1.	Functionality	The bidder to propose relevant SAN switch for the SAN storage in redundant high availability.
2.		Necessary software to configure and manage the storage space, RAID configuration, logical drives allocation, virtualization, snapshots for entire capacity etc. should be included.
3.		Should support Non-disruptive component replacement of controllers, disk drives, power supply, fan subsystem etc.
4.		Should support the supplied storage and operating systems.
5.		The storage should support all the Operating System Platforms & Clustering
6.		Any software or license required to enable connectivity to these OS / software should be included.
7.		Storage should support non-disruptive online firmware upgrade for both controllers and disk drives.
8.		Should be able to support clustered and individual servers at the same time.
9.		Should come equipped with storage management software for configuration and patching.
10.		Should support automated SAS storage tier feature across the populated drives.
11.		The storage system shall be configured with GUI based management software as below:

Sr. No.	Component	Requirement description
		• Monitor and manage the storage array Configuration. • Remote Storage base replication. • Storage front end port monitoring. • Disk Monitoring. • LUN management. • Storage Component replacement, etc.
12.	Technical specification*	Usable storage capacity of minimum 200 TB from Day 01 and scalable up to 1 PB.
13.		Should support hot plug and hot swap of components online (including controllers, power supplies, cooling fans etc.)
14.		Should have redundant controller, power and cooling.
15.		The storage system should be scalable.
16.		Should provide LUN masking, fiber zoning and SAN security.
17.		All relevant software required should be in-built.
18.		Should be equipped with hot spares.
		Should support remote replication and replication license included.
19.		Synchronous and Asynchronous replication support should be available with relevant licenses.
20.		Should support FC, iSCI protocols. BIS compliant and registered.
21.		Should be IPV6 ready from Day 01 of installation.

***Note:**

1. The bidder has to assess and propose SAN switch as per requirement in high availability.
2. Storage requirement is for data retention for a period of 01 year which may be updated later as per OCAC data retention policy. Any additional storage requirement cost would be as per the financial proforma as quoted by the bidder.
3. The bidder to assess the infrastructure and proposed relevant drive capacity and number of slots as per the scalability and storage requirement.

7.11 Vulnerability Management Solution

Sr. No.	Component	Requirement description
1.	Functionality	The OEM of the solution should be in the Gartner, Forrester, IDC, NSS, etc. leader quadrant in the latest reports.
2.		The solution must be completely on premise solution.
3.		Bidder to propose and implement virtual machine for deployment of Vulnerability Management Solution.
4.		Solution should have Self-signed certificate generation features so that accessing of appliance from client for monitoring and administration purposes can be done in encrypted manner.
5.		Solution should be IPv6 ready from day one to integrate with full IPv6 network.
6.		Vulnerability management solution should be a dedicated solution and not part of SIEM.
7.		Vulnerability management solution should be based on 512 floating IP addresses (IPs can be changed and active scanning can be done as per requirement) from Day 01 and can be increased as per requirement.
8.		Integrates seamlessly with the SIEM.

Sr. No.	Component	Requirement description
9.		Ability to import vulnerability assessment and scan results sources for centralized reporting, dash boarding and analysis.
10.		Is able to transparently utilize all existing points of presence for scanning purposes as possible.
11.		Is CVE compliant and provides vulnerability risk scoring based on accepted industry standards (CVE,CVSS);
12.		Can orchestrate a high volume of concurrent assessments without disturbing normal network operations (customizable bandwidth usage);
13.		Can scan both external facing and internal IP ranges;
14.		Can scan in zero privileged or credentialed mode;
15.		Can perform privileged scanning of network devices;
16.		Can scan virtual hosts;
17.		Provides a flexible and automated remediation assignment capability;
18.		Provides easy access to the solution through a web based interface;
19.		Delivers role based reporting and operational functionality through a cascading permissions structure so each user has personalized information based on their role and the assets they are responsible for managing;
20.		Allows multiple stakeholders to scan and rescan (for remediation verification) as needed;
21.		Provides flexible assessment scheduling options;
22.		Enforces approved time windows for scans and automatically manages scans across windows (pause and re-start);
23.		Allows for acceptable risks and false positives to be exceptional from reporting and workflow based on customer defined business rules;
24.		Captures an audit trail associated with all activities (e.g. discovery, assignments, notes, exceptions, remediation etc.) vulnerabilities;
25.		Generates alerts and reports on newly emerging vulnerabilities in between scans, using passive correlation;
26.		Differentiates between active and inactive IP addresses
27.		Enables access to raw scan and report data (custom report building).
28.		Create, manage and schedule vulnerability scans View and report on vulnerability scan results;
29.		The Solution must provide the ability to produce ad hoc reports while viewing results in the console. PDF and CSV exports shall be available.
30.		Efficiently manage detected vulnerabilities, through a series of powerful vulnerability views and the application of very flexible vulnerability filtering; enabling users to focus on the key, must fix vulnerabilities;

7.12 Network Monitoring, Helpdesk and Ticketing tool

Sr. No.	Component	Requirement description
1.	Functionality	The network monitoring tool must monitor performance across heterogeneous networks from one end of the enterprise to the

Sr. No.	Component	Requirement description
		other.
2.		Proposed NMS solution must be ISO 27001 certified to ensure security compliances.
3.		NMS OEM must be an industry standard solution and shall be in the present for NPMD and ITSM both in latest published Gartner's MQ reports and leading analysts' reports like IDC or Forrester.
4.		Proposed NMS solution MUST have at least 2 deployments in Indian Government/ Public Sector, monitoring & managing 2500+ network nodes in each of such deployments. Customer names, solution details and OEM undertaking needs to be provided at the time of bidding.
5.		OGC Gold level or Pink Elephant certifications for ITILv3 in at least 10+ processes or equivalent.
6.		The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.
7.		The proposed solution should also provide network asset inventory reports.
8.		The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e. Router, Switches, Servers, etc.) and map the connectivity between them with granular visibility up to individual ports level.
9.		The tool shall be able to assign different icons/ symbols to different type of discovered elements. It should show live interface connections between discovered network devices.
10.		Should support manual addition and deletion of devices from the repository of assets in the tool.
11.		It should support various discovery protocols to perform both manual and automatic discovery of all L2, L3 Network devices across any network connectivity existing or planned in future.
12.		In case of dual stack devices, the system shall be able to discover and show both IPv4 and IPv6 IP addresses.
13.		It shall provide an option to discover and manage the devices/elements based on SNMP as well as ICMP.
14.		The proposed Network Fault Management solution must support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP Trap based discovery.
15.		It must also allow for inclusion and exclusion list of IP address or devices from such discovery mechanisms.
16.		The proposed solution must provide a detailed asset report, organized by vendor name, device type, listing all ports for all devices.
17.		The Solution must provide reports to identify unused/dormant network ports in order to facilitate capacity planning.
18.		The system should be able to clearly identify configuration changes / policy violations / inventory changes across multi-vendor network

Sr. No.	Component	Requirement description
		tool.
19.		The system should support secure device configuration capture and upload and thereby detect inconsistent "running" and "start-up" configurations and alert the administrators.
20.		The proposed fault management solution must able to perform "load & merge" configuration changes to multiple network devices.
21.		The proposed fault management solution must able to perform real-time or scheduled capture of device configurations.
22.		Should able to support and handle large volume of incident, service requests, changes, etc.
23.		The solution should have a Single Architecture and leverage a single application instance across ITIL processes.
24.		Support unique data and workflows segregated user role for Incident, Problem, Change, Release, Knowledge Management, Asset Management and CMDB
25.		Should provide out-of-the-box categorization, as well as routing and escalation workflows that can be triggered based on criteria such as SLA, impact, urgency, CI, location or department.
26.		Should support customization of severity level as per requirements.
27.		Multiple instances shall be allowed to be configured in different ways in different modules for different outcomes.
28.		The tool should have the knowledge management OOB – knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions.
29.		Should allow creating and applying various operational level parameters to Incidents, Requests, Changes, and Release management modules.
30.		Should have a predefined/customizable field to indicate & track the progress/status of the lifecycle of ticket(s).
31.		The solution should support SLA violations alerts during the tracking period.
32.		The tool should provide an audit trail, tracking & monitoring for record information and updates from opening through fulfilment to closure.
33.		The solution should support managing and maintaining a full history of an incident SLA.
34.		Should use Industry-standard protocols such as WMI, SNMP, JMX, SSH to perform discovery without requiring the installation of an agent.
35.		Should have ability to modify out-of-box discovery scripts, create customized discovery scripts
36.		Discovery should work without requiring agent installation (that is, agent-less discovery) while discovery Layers 2 through Layers 7 of OSI model
37.		The tool shall be able to work on SNMP V-1, V-2c & V-3 based on the SNMP version supported by the device.
38.		The solution should have internal storage and function without any third party database.
39.		The solution should be able to integrate with SOAR solution.
40.		The Helpdesk and ticketing system should store unlimited number of incidents.

Sr. No.	Component	Requirement description
41.		The solution should have manual or automated escalation mechanism for incidents.
42.		Should support configuration for auto escalation of tickets during SLA violations.
43.		The solution should support at least 2 administrator user accounts and at least 10 user accounts.
44.		The solution should be able to store incident records for a period of at least 90 days.
45.		Should have provision to archive data for future reference and retrieval.
46.		The tool shall be able to discover IPv4 only, IPv6 only as well as devices in dual-stack.
47.		Should be able to generate reports regarding CPU and memory utilization for routers, switches and servers.

7.13 Desktop

Sr. No.	Component	Requirement description
1.	Functionality	Desktop should be preloaded with suitable operating system which may provide ease of operations.
2.		Operating system should be of the latest configuration and enterprise version.
3.		Desktop should be of the latest model and configuration.
4.		Desktop should be available with proper accessories for installation.
5.		All the components of the desktop (like keyboard, mouse, etc.) should be of the same OEM.
6.		Monitor should emit minimal radiation for lesser eye strain.
7.		Monitor should have minimum border bezel width.
8.	Technical specification	Intel i5 processor with 6 cores per processor, 2.8 GHz base frequency and 9MB cache memory
9.		Have an additional 1 PCI slot
10.		Integrated graphics – Intel HD 630
11.		OS partition and storage should be in local hard drive.
12.		Minimum 8GB RAM DDR4 with 2666 MHz speed
13.		Additional 01 number of DIMM slots should be present
14.		Should have a hard drive capacity of 1000 GB @ 7200 rpm
15.		Should have an optical drive DVD R/W
16.		Audio in & out, Headphone and microphone ports should be present.
17.		Should have minimum 2 number of 10/100/1000 on board Integrated Gigabit Port
18.		Should have minimum 4 number of USB 3.0 ports
19.		Should have minimum 02 number of VGA ports for two display connections.
20.		Keyboard should be standard type with USB connector.
21.		Mouse should be optical scroll wired
22.		Mouse connector should be USB type
23.		**Monitor:**
24.		Monitor should be 27 inches diagonally in size with aspect ratio 16:9
25.		Monitor should bear resolution of 1920x1080 pixels
26.		Screen should be curved with screen curvature of 1800R

Sr. No.	Component	Requirement description
27.		Dimension should not be greater than 615 x 458 x 271 mm
28.		Monitor should be LED backlit
29.		Should have minimum 01 number of VGA display port and 01 number HDMI port
30.		Native contrast ratio should be at least 3000:1
31.		Should have a response time of maximum 5 millisecond
32.		Viewing angle should be 178 / 178
33.		Monitor screen should be coated with anti-glare
34.		Desktop should have power consumption of 180W with 90-95% efficiency
35.		Should be RoHS / Energy star compliance equipment

7.14 Multifunction Printer

Sr. No.	Component	Requirement description
1.	Functionality	The printer should be laser jet.
2.		Should have duplex print feature
3.		Should support print through wireless direct print connection
4.		Should support only black and white printing
5.		Should have features for print, copy and scan.
6.		Copier should take input from the flatbed scanner.
7.		Table top or stand mountable
8.		Plug and play driver installation
9.		Equipment should be from a brand with best service life hours
10.	Technical specification	Print speed up to 30 ppm
11.		Support resolution up to 1200 x 1200 dpi
12.		Should support driver installation in all operating systems
13.		Scanner Flatbed type with CIS technology
14.		Scanner support file format like PDF, JPEG, PNG
15.		Front-panel scan, copy buttons
16.		24 bit scan depth with 256 greyscale levels
17.		Copy speed up to 30 cpm
18.		Copier support resolution of 300 x 300 dpi
19.		Copier support enlargement of image from 25 to 400%
20.		Copier should support extended contrast adjustments
21.		Connectivity ports: 1 Hi-Speed USB 2.0 Device; 1 Hi-Speed USB 2.0 Host; 1 Fast Ethernet 10/100Base-TX; 1 Wireless 802.11b/g/n
22.		Memory 256 MB with 750 MHz processor speed
23.		Supports minimum duty cycle of 65000 pages monthly basis
24.		Input / output 350 sheets (standard), 100-sheet multipurpose tray, 250-sheet input tray; 250-sheet output bin
25.		Support media type A4; A3; B4 (JIS); B5 (JIS); A5; 16K
26.		Support fonts and typefaces PCL 84 fonts; PCL 6 84 fonts; Postscript 83 fonts
27.		Control panel 3.0-in; 320 x 240 pixel backlit graphical display; touchscreen; buttons (Home, Cancel, Help, Right/Left Arrows, Back); LED indicator lights (Ready, Error, Wireless)
28.		3.0-in Touchscreen, LCD (colour graphics)
29.		Security features: SNMP v3, SSL/TLS (HTTPS), 802.1x authentication; password protection, WPA (Wi-Fi Protected Access), WEP encryption, 802.1x authentication

8. Manpower for CSOC

8.1 Manpower requirement

Sr. No	Manpower Designation	No. of resource
1	SOC manager	1
2	Security administration and Threat Intelligence expert	1
3	SOC Engineer	3
4	SOC Level 2 Analyst	7
5	SOC Level 1 Analyst	7
6	Receptionist	1
	TOTAL	**20**

Sr. No	Manpower Designation	Shift details
1.	SOC Manager	• General shift: All days of week except Sunday / State Government holidays. • Time: 10:00 am to 06:00 pm
2.	Security Threat and Intelligence Expert	• General shift: All days of week except Sunday / State Government holidays. • Time: 10:00 am to 06:00 pm
3.	SOC Engineer	• Minimum 1 resource available during the time specified. • All days of week with shift rotation. • Time: 09:00 am to 09:00 pm
4.	SOC Level 2 Analyst	• Minimum 2 resource available during the time specified. • All days of week with shift rotation. • 24*7 onsite management on shift basis
5.	SOC Level 1 Analyst	• Minimum 2 resource available during the time specified. • All days of week with shift rotation. • 24*7 onsite management on shift basis
6.	Receptionist	• General shift: All days of week except Sunday / State Government holidays. • Time: 10:00 am to 06:00 pm

Note:

1. The above table is indicative only. The bidder can propose a shift rooster as per his own convenience and optimal utilization of resources.
2. In any case of emergency or urgent leave, an equivalent replacement should be present with prior approval from department SPOC / Nodal officer.
3. During any critical incident, manpower should be available even beyond the specified working hours.
4. On a non-working days and government holidays, minimum 05 manpower resources should be available at the CSOC with respect the working shifts mentioned.

8.2 Manpower qualification

Curriculum vitae / resume of manpower should be submitted together with the technical proposal by the bidder to OCAC as per the below mentioned requirement / qualification.

Sr. No.	Designation of Manpower	Qualification required
1.	Level 1 Analyst	• B.E / B-Tech /MCA • Minimum of 3 years of experience in SOC services through on-premises or managed mode of service provider. • Minimum 2 year experience in operating a SIEM product and other security tools. • Have experience in handling log management and incident management. • CEH certified preferred.
2.	Level 2 Analyst	• B.E. / B-Tech / MCA • Total 6 Years of experience out of which, minimum 4 years of experience in SOC services conducting security device administration & management and minimum 2 years in SIEM tool & other security tools. • Certification in at least one industry leading SIEM product. • Certifications in security, such as CISA, CEH, CISSP, CISM, CRISC (any one) preferred. • Certification in ISO 27001:2013 or later version.
3.	CSOC Engineer	• B.E / B-Tech / MCA / Diploma in relevant field. • Minimum of 3 years of experience in security device administration & management. • Have experience in vendor management, patch management, Helpdesk and incident management. • Certified in ITIL v3 or later version. • ISO 27001:2013 or later version certification preferred.
4.	Security Administration and Threat Intelligence expert	• B.E / B-Tech/MCA • Minimum 8 years of experience out of which, minimum 5 years relevant experience in SOC services, SOC administration, threat analysis and hunting, SOC configuration and management. • Certification in security CISA, CEH, CISSP, CISM, CRISC (any one). • Certification in ISO 27001:2013 or later version. • Certification in CTIA from a recognized body is preferable.
5.	SOC Manager	• B.E / B-Tech with MBA • Minimum 10 years of experience out of which, minimum 6 years relevant experience in management from reputed organizations. • Must have experience of 2 to 3 years with a cybersecurity domain project and associated with a cybersecurity organization. • Certification in PMP, PRINCE2, CPMP, PgMP, CSM etc. (any one).
6.	Receptionist	The bidder to propose a suitable and experienced candidate for the required position.

8.3 Manpower roles and responsibilities

Sr. No.	Designation of Manpower	Roles and Responsibilities

Sr. No.	Designation of Manpower	Roles and Responsibilities
1.	Level 1 Analyst	• Level 1 analyst will identify, categorize, prioritize, and investigate events rapidly utilizing triage and response guidelines for the enterprise using commonly available CSOC log sources that include: ➢ Firewalls and network devices. ➢ Infrastructure server and end-user systems. ➢ Threat intelligence platforms. ➢ Web proxies. ➢ Application logs and web-application firewalls. ➢ Identity and access management systems. ➢ Cloud and hybrid-IT provisioning, access, and infrastructure systems. ➢ Antivirus systems. ➢ Intrusion detection and prevention systems. • Monitor incoming event queues for potential security incidents. • Perform initial investigation and triage of potential incidents, and escalate or close events as applicable. • Monitor CSOC ticket (or email) queue for potential event reporting from outside entities and individual users. • Maintain CSOC shift logs with relevant activity from the shift. • Document investigation results, ensuring relevant details are reported to level 2 analyst for final event analysis. • Update or refer CSOC collaboration tool as necessary for changes to CSOC process and procedure as well as ingest CSOC daily intelligence reports and previous shift logs. • Conduct security research and intelligence gathering on emerging threats and exploits. • Perform additional auxiliary responsibilities as outlined in the console monitoring procedure. • Communicating emergency alerts & warnings to designated stakeholder/ departments/ OCAC.
2.	Level 2 Analyst	• Monitor level 1 analyst performance by investigating incoming events using CSOC-available tools. • Ensure level 1 event(s) are addressed in a timely manner using available reporting and metrics. • Approve and, if necessary, further investigate level 1-escalated events. • Mentor level 1 analysts to improve detection capability within the CSOC. • Manage CSOC event and information intake to include gathering intelligence reports, monitoring ticket queues, investigating reported incidents, and interacting with other security and network groups as necessary. • Serve as detection authority for initial incident declaration. • Function as shift subject-matter experts on incident

Sr. No.	Designation of Manpower	Roles and Responsibilities
		detection and analysis techniques, providing guidance to junior analysts and making recommendations to organizational managers. • Drive and monitor shift-related metrics processes ensuring applicable reporting is gathered and disseminated per CSOC requirements. • Conduct security research and intelligence gathering on emerging threats and exploits. • Serve as a backup analyst for any potential coverage gaps to ensure business continuity. • SOC Performance Monitoring.
3.	CSOC Engineer	• Responsible for infrastructure deployment and upkeep and content development. • Develop, implement, and execute the standard procedures for the administration, backup, disaster recovery, and operation of the CSOC systems infrastructure, including: ➢ Operating system security hardening ➢ Backup management ➢ Capacity planning ➢ Change management ➢ Version or patch management ➢ Lifecycle upgrade management ➢ Configuration management • Develop and maintain the technical architecture of the CSOC system, enabling all the components to perform as expected and meeting established service-level objectives for system uptime. • Perform routine equipment checks and preventative maintenance. • Maintain up-to-date documentation of designs or configurations. • Respond to after hours (on-call support) infrastructure issues as required. • Be responsible for new product release management, policy and integration testing, security testing and vendor management. • Maintain hardware or software revisions, SIEM content, security patches, hardening, and documentation. • Develop and deploy content for the CSOC infrastructure, including use cases for dashboards, active channels, reports, rules, filters, trends, and active lists. • Monitor and help optimize data flow using aggregation, filters, and use cases to improve the CSOC monitoring and response capabilities. • Coordinate and conduct event collection, log management, event management, compliance automation, and identity monitoring activities.

Sr. No.	Designation of Manpower	Roles and Responsibilities
		• Respond to day-to-day security change requests related to CSOC operations. • Perform collateral duties and responsibilities as a backup to the security engineering role.
4.	Security Administration and Threat Intelligence expert	• Reviews asset discovery and vulnerability assessment data. • Review standard security arrangements, provide external/semi-external reviews. • Explores ways to identify stealthy threats that may have found their way inside network, without detection, using previous experience in threat intelligence. • Conducts vulnerability and penetration tests on production systems to validate resiliency and identify areas of weakness to fix. • Investigate new vulnerabilities and share the latest industry level responses. • Recommends how to optimize security monitoring tools based on threat hunting discoveries. • Incident Forensic handling and analysis. • Network and security consulting and training. • Risk assessment and mitigation. • Liaise with different internal and external stakeholders when an incident occurs • Manage remotely stored critical information (passwords, network configurations, etc.) during any high level incident.
5.	SOC Manager	• Manager is responsible for achieving the goals of the CSOC program through the implementation of processes, procedures, and performance indicators related to security incidents and prevention management. • SOC manager would be responsible for maintaining smooth operations, ensuring service-level agreements (SLAs) are met. • Manage the overall day-to-day operations. They are responsible for ensuring events and/or incidents are detected and responded to in adherence to established process as well as procedures. • Oversee the analysts' daily tasking. • Manage the team's work scheduling. • Ensure effective incident management. • Identify chronic operational and security issues, and ensure they are managed appropriately. • Manage and escalate roadblocks that may jeopardize security monitoring operations, infrastructure and SLAs. • Serve as a senior mentor to CSOC staff. • Interface and collaborate with outside teams. • Track tactical issues in execution of CSOC responsibilities.

Sr. No.	Designation of Manpower	Roles and Responsibilities
		• Document and track analyst training requirements. • Ensure analysts follow existing procedures and all procedures are documented in accordance with local guidelines. • Manage the process improvement program for CSOC processes. • Serve as an incident manager for the CSOC, along with other responsibilities. • Provide security advisor to OCAC/departments on timely basis. • Creation of reports, dashboards for CSOC operation and reporting to OCAC on weekly basis.

8.4 Additional Manpower requirement

In situations where any severe breach or security incident had occurred in the State of Odisha, additional manpower may be hired on temporary basis for investigation and root cause analysis. The additional manpower is irrelevant of the scope of the bidder and on need basis only. The scope of the additional manpower may be decided when and where the need arises and would be duly communicated.

Sr. No	Manpower description	Manpower quantity	Qualification required
1	Forensic Analyst	As per requirement on request from OCAC	• Should have a valid forensic analyst certification. • Minimum 05 years of experience of functioning as a digital forensic analyst or associate. • Have hands on experience in handling forensics on computer systems, storage devices, digital documents & files, network & security equipment, etc.
2	Threat Hunting Specialist	As per requirement on request from OCAC	• Minimum 10 years of experience in Security Operations Centre (SOC) or Cyber security domain. • Have knowledge about all the solutions implemented in SOC. • Have minimum 3 years of experience as a red team or blue team member. • Must have scripting knowledge and not totally depend on automated solutions.
3	Security trainer	As per requirement on request from OCAC	• Minimum 10 years of experience with any security solution OEM. • Have relevant knowledge with security solution at different level of security architecture. • Have hands on experience with security solution interface and configurations. • Have experience in providing security related training and conferences to

Sr. No	Manpower description	Manpower quantity	Qualification required
			enterprises for cyber risk related matter and technology.

9. Service Level Agreement

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

- **"Availability"** shall mean the time for which the services and facilities offered by the implementation agency are available for conducting operations from the equipment installed.

- "**Downtime**" is the time the services and facilities are not available, which excludes the scheduled outages planned in advance.

- "**Helpdesk Support**" shall mean the implementation agency's 24x7x365 Helpdesk Support Centre which shall handle incident reporting, trouble handling, ticketing and related enquiries during this engagement.

- "**Incident**" refers to:
  - Any event / abnormalities in the functioning of the SOC equipment / services that may lead to disruption of SOC services.
  - Any security compromise or vulnerability observed in the client infrastructure.

  Incidents are classified into different severity level based on the impact of the incident:

Sr. No.	Severity	Incident classification
1.	Critical	a) Incidents, whose resolution shall require additional investment in component or time or shall involve co-ordination with OEMs. These incidents shall impact the overall functioning of the SOC. For example: device failure, device module failure, port failure, etc. The SLA would be measured for the time taken to bypass the device, establish logical redundancy and restore rest of the services of CSOC. b) Any security incident occurred / vulnerability found, bearing impact to disable the operations of a whole department / stakeholder. c) Any incident reported by department where a breach had already occurred.
2.	High	a) Incidents, whose resolution require change in the architecture / design / configuration of the SOC components. b) Integration issue with any department / stakeholder infrastructure. c) Any security incident / vulnerability found bearing impact to disrupt the operation of any asset and limited to that asset only (example: network device, server, website, etc.). The SLA would be measured as per the time taken to isolate the device from the network without disrupting the rest of the operations of CSOC. d) Incidents arising due to power UPS / DB / electrical fault

Sr. No.	Severity	Incident classification
		which can impact the services of SOC and its components. e) Any other incident having an impact on the services provided by SOC.
3.	Medium	a) Incidents, whose resolution require software upgradation / patch management for the SOC infrastructure but have no serious impact on the stakeholder's infrastructure. b) Any security incident / vulnerability found bearing no current impact on the stakeholder infrastructure but may arise as a serious threat in future. c) Incidents related to CCTV, access control, etc. which bear no impact on the services of SOC. The response timelines for these items / parameters should be as per individual SLA defined.
4.	Low	a) Alerts / events reported by the SOC infrastructure which may be doubtful in nature as false positive and requires further investigation. b) Incident bearing no threat but only to be circulated as awareness and information / advisory to all stakeholders. c) Any security threat / update provided by recognized bodies (e.g. CERT-In, NIST, etc.) for inclusion in SOC as best practises. d) Incidents related to SOC civil and electrical works, power, alarm system, etc. which bear no impact on the services of SOC. The response timelines for these items / parameters should be as per individual SLA defined.

Note:

a. The critical and high incident should be analysed and root cause analysis for the same should be provided by the successful bidder for every such incident.
b. Any incident which is out of scope or dependent on other stakeholders / department should be released from isolation with relevant approval from OCAC / CERT-O.
c. Any incident where replacement / procurement /upgradation of asset is required, the successful bidder should obtain proper approval from OCAC for relaxation of SLA. Proper cause of relaxation requirement along with the actual timeline required to be submitted by the successful bidder to OCAC. Any deviation from the actual timeline provided would be penalized as per SLA for Supply, Installation and Commissioning & Testing.

- "**Resolution Time**" means time taken by the bidder to troubleshoot and fix the problem from the time the incident had been reported or the incident has been logged at the Helpdesk (whichever is earlier) till the time the problem has been fixed.

9.1 Service level parameters

9.1.1 Device and software availability

- All the devices / appliances in form of hardware should maintain a minimum uptime of 99.90% over the measurement period mentioned.
- The uptime of devices is not limited to hardware only but also software, operating system, virtual environment, etc.
- The device availability would again be segregated as per the device placement and functionality:
  - The uptime of SOC devices (example: switch, Anti-APT, SAN switch, SAN, Log appliance, etc.) should be taken as a whole and the SLA would be calculated as the average of the devices uptime.
  - The uptime of software / applications should be considered as a different component and the SLA would be measured likewise.
  - The surveillance (CCTV) uptime would be calculated as a separate parameter.
  - The UPS set uptime and load output would be taken as separate parameter for calculation of SLA.
  - Any incident related to civil work would be taken as a separate parameter for SLA measurement.

Sr. No.	Definition	Measurement Interval	Target
1.	Device uptime / Device availability	Monthly	>=99.90%
2.	SOC application / software availability	Monthly	>=99.90%

9.1.2 Incident logging and Response

- Every incident whether reported as alerts or notifications by the SOC devices or reported by the department / officials should be logged without fail.
- Resolution to every incident should be provided as per the SLA target mentioned.
- The number of hours and days mentioned in SLA are inclusive of office working or non-working time period. Any escalation to be made outside the working hours should be done through both written and telephonic communication.
- Any vulnerability recognised during vulnerability assessment should also be considered as an incident.
- Any critical incident where additional investment or replacement of asset is required is also to be logged.

Sr. No.	Definition	Measurement Interval	Target
1.	Incident Logging	Monthly	• 100% logging of all alerts and security incidents. • 100% logging of all department / official reporting of incidents.

Sr. No.	Definition	Measurement Interval	Target	
2.	**Incident response**			
a.	**Scenario 1: When the bidder has full control and authority for the mitigation of the incident**			
i.	Critical	Monthly	Mitigation of incident - Less than the next 3 hours	
			Timeline for isolation of the threat or vulnerability through CSOC operations / bypass of the system – the next 30 minutes.	
			Timeline for identification of the vulnerability / cause of incident – 30 minutes.	
ii.	High	Monthly	Mitigation of incident - Less than the next 6 hours	
			Timeline for isolation of the threat or vulnerability through CSOC operations / bypass of the system – the next 1 hour.	
			Timeline for identification of the vulnerability / cause of incident – 1 hour.	
iii.	Medium	Monthly	Less than 3 days	
iv.	Low	Monthly	Less than 7 days	
b.	**Scenario 2: When the bidder is dependent on other Stakeholders (OCAC, OSDC, OSWAN, Odisha State IT centre, Other departments under CSOC) for mitigation of incident**			
i.	Critical	Monthly	Level 3 escalation to OCAC and the concerned department / stakeholder	Within 12 hours of second escalation
			Level 2 escalation to OCAC and the concerned department / stakeholder	Within 8 hours of first escalation
			Level 1 escalation to OCAC and the concerned department / stakeholder.	Within 3 hours
			Timeline for isolation of the threat or vulnerability through CSOC operations / bypass of the system and escalation to concerned department / stakeholder	The next 30 minutes

Sr. No.	Definition	Measurement Interval	Target	
			Timeline for identification of the vulnerability / cause of incident	30 minutes
ii.	High	Monthly	Level 3 escalation to OCAC and the concerned department / stakeholder	Within 24 hours of second escalation
			Level 2 escalation to OCAC and the concerned department / stakeholder	Within 12 hours of first escalation
			Level 1 escalation to OCAC and the concerned department / stakeholder.	Within 6 hours
			Timeline for isolation of the threat or vulnerability through CSOC operations / bypass of the system and escalation to concerned department / stakeholder	The next 1 hour
			Timeline for identification of the vulnerability / cause of incident	1 hour
iii.	Medium	Monthly	Level 3 escalation to OCAC and the concerned department / stakeholder	Within 72 hours of second escalation
			Level 2 escalation to OCAC and the concerned department / stakeholder	Within 48 hours of first escalation
			Level 1 escalation to OCAC and the concerned department / stakeholder.	Within 48 hours
iv.	Low	Monthly	Level 3 escalation to OCAC and the concerned department / stakeholder	Within 07 days of second escalation
			Level 2 escalation to OCAC and the concerned department / stakeholder	Within 03 days of first escalation
			Level 1 escalation to OCAC and the concerned department / stakeholder.	Within 4 days

Note:

1. All timelines are to be considered from the point of occurrence of the incident / generation of alerts / information received from any external agency or stakeholder.
2. For every incident logged under "Scenario 2", after Level 3 escalation SLA would not be applicable to the bidder.
3. For every incident logged under "Scenario 2", bidder would provide root cause analysis and mitigation recommendation during Level 2 escalation to the respective stakeholder / department.

Escalation matrix

The escalation matrix defines who is responsible at what level for handling any incident or situation in an organization. The matrix below would define the timeline for escalation and the way thereafter for different stakeholders for the project with Level 1 being the lowest level of escalation.

For the project sponsoring authority / OCAC:

Sr no.	Level of escalation	Personnel designation	Escalation timeline
1.	Level 3	Chief Executive officer – OCAC	As per SLA defined.
2.	Level 2	General Manager (Admin)	As per SLA defined.
3.	Level 1	SPOC assigned by the department	As per SLA defined.

For the respective stakeholder:
The personnel are to be nominated by the respective stakeholder at a later stage.

9.1.3 Manpower availability

- Manpower is a critical aspect of the project and no absence or deviation from the SLA would be acceptable.
- In case absence could not be avoided by the bidder, additional manpower of the same skill level and designation should be stationed at the client premises on temporary basis.
- SLA for manpower availability to be maintained at all times.

Sr. No.	Definition	Measurement Interval	Target
1.	Manpower availability	Monthly	100% attendance as per defined in Section 8.1 of the RFP document.

9.1.4 Surveillance and monitoring

- The CCTV monitoring should not be down at any time at any day.
- The CCTV monitoring should run 24*7*365 with all the cameras in active condition at all times.
- The CCTV footage should be stored in the local device storage and should be transferred to an external storage when and where required.
- At least 60 days CCTV footage should be stored by the bidder (device storage or external storage). The extended footage could be written in the storage space.

Sr. No.	Definition	Measurement Interval	Target
1.	Surveillance and monitoring	Monthly	• 24*7*365 uptime of all CCTV cameras. • 60 days continuous recording of CCTV footage. • Archival of CCTV footage for one year (not applicable for the first year).

9.1.5 Business Continuity Plan testing

- The bidder has to submit a BCP plan to OCAC within the first year of operations. The BCP plan and activities should be reviewed and approved by OCAC.
- The bidder every year once would implement a BCP drill to test the redundancy and point of failure in the SOC design / architecture.
- The BCP testing would be done for devices in high availability, network as redundancy and services as redundancy.
- The BCP testing would include the testing of the fire alarm system, mock fire drill and access control system.

Sl. No.	Definition	Measurement Interval	Target
1.	Business Continuity Plan testing	Yearly	A BCP drill should be conducted once every year (with minimum gap of six months from previous BCP drill) to test the redundancy and point of failures in the SOC design.

9.1.6 Electrical power and backup

- UPS would be installed in N+N redundant mode for uninterrupted power backup function. Both of the UPS should be fully functional and operational 24*7*365 in master slave mode.
- Power distribution should be operational without any fault at all times.

Sl. No.	Definition	Measurement Interval	Target SLA
1.	Electrical power and back up		
(a)	Power DB	Monthly	Resolution to incident less than 4 hours
(b)	UPS		Resolution to incident less than 12 hours

9.1.7 Access control

- Access control should be connected to power backup systems to be operational even during main power down scenarios.
- All logs of access control should be captured for future references whenever required.
- The access control should be operational at all times.

Sl. No.	Definition	Measurement Interval	Target SLA
1.	Access Control	Monthly	100% operational 24*7*365

9.1.8 Fire alarm and rodent repellent

- The fire alarm system should be operational at all times.
- The system would be tested during BCP testing yearly.
- Rodent repellent system should be operational at all times.

Sl. No.	Definition	Measurement Interval	Target SLA
1.	Fire alarm	Monthly	100% operational 24*7*365
2.	Rodent repellent	Monthly	100% operational 24*7*365

9.1.9 Civil and electrical works

- All incidents related to civil and electrical works should be resolved by the bidder during the operations and maintenance period.
- If any external vendor needs to be hired (example: electrician, mechanic, etc.), that would be done by the bidder itself. All cost of the repair would be borne by the bidder.
- Civil and electrical works would be but not limited to: Ceiling, flooring, light fixtures, cabling, etc.

Sl. No.	Definition	Measurement Interval	Target SLA
1.	Civil works	Monthly	100% operational 24*7*365
2.	Electrical works	Monthly	100% operational 24*7*365

10. Project Timelines

The start date of the project shall be from the date of signing the contract / agreement for the engagement.

T0- Represents the Project Start Date (i.e. agreement signoff date).

Sr. No.	Activity	OCAC	PMU	IA	Timeline	Remarks
1	MSA signing between OCAC and IA	√		√	T0	Kick-off meeting to happen within a week from the date of LoI along with signing of MSA between the two parties.
2	Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval	√	√	√	T0 + 4 weeks	Submission of design documents, layout, drawing etc. for statutory approvals.
3	Finalization and Approval of the submitted layout, etc.	√	√	√	T0 + 6 weeks	IA has to work with OCAC for approval of submitted drawings and layout.
4	Completion of Structural, Architectural, Civil & Interior Works.		√	√	T0 + 16 weeks	Completion of all Civil and Interior works and inspection report of all item delivered & erected. Successful bidder shall furnish weekly progress report.
5	Supply, Installation and Commissioning & Testing of all Non-IT asset.		√	√	T0 + 22 weeks	Successful bidder shall carry out integrated system testing of all equipment and rectify all snags.

Sr. No.	Activity	OCAC	PMU	IA	Timeline	Remarks
	Supply, Installation and Commissioning of all IT Equipment					Consultant to work with successful bidder for User acceptance Test sign-off of Non-IT Infrastructure system from OCAC
6	Project Sign-Off & FAT (Go-Live of the Project)	√	√	√	T0 + 24 weeks	Successful Final Acceptance Test of all commissioned IT and Non-IT systems and Issue Go-Live Certificate from OCAC
7	CSOC - Operations and Maintenance Phase	√	√	√	4 years from the date of CSOC Go-Live	The initiation date of O&M phase would be from the date of Go-Live certificate issued from OCAC. The O&M phase would continue for a period of 4 years from the date of Go-Live.

11. Payment terms

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

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

Sr. No.	Activity	Payment	Remarks
1	Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval	80% of the quoted cost for the activity (civil and interior works)	Submission of design documents, layout, drawing etc. for statutory approvals.
2	Finalization and Approval of the submitted layout, Floor diagram, Non-IT and IT architecture, etc.		IA has to work with OCAC for approval of submitted drawings and layout.
3	Completion of Structural, Architectural, Civil & Interior Works.		Completion of all Civil and Interior works and inspection report of all item delivered & erected. Successful bidder shall furnish weekly progress report.
4	Supply of all Non-IT asset. (excluding the civil and interior works)	20% of quoted cost by the bidder for Non- IT items (excluding the civil and interior works)	Successful bidder shall share all itemized delivery details and challans related to the assets. Consultant to work with successful bidder for verifying the supply sign-off of Non-IT Infrastructure system from OCAC

Sr. No.	Activity	Payment	Remarks
5	Installation and Commissioning & Testing of all Non-IT asset. (excluding the civil and interior works)	60% of quoted cost by the bidder for Non- IT items (excluding the civil and interior works)	Successful bidder shall carry out integrated system testing of all equipment and rectify all snags. Consultant to work with successful bidder for User acceptance Test sign-off of Non-IT Infrastructure system from OCAC
6	Supply of all IT asset	20% of the quoted cost by the bidder for IT items	Successful bidder shall share all itemized delivery details and challans related to the assets. Consultant to work with successful bidder for verifying the supply sign-off of IT Infrastructure system from OCAC
7	Installation and Commissioning of all IT asset	60% of the quoted cost by the bidder for IT items	Successful bidder shall carry out integrated system testing of all equipment and rectify all snags. Consultant to work with successful bidder for User acceptance Test sign-off of IT Infrastructure system from OCAC
8	Project Sign-Off & FAT (Go-Live of the Project)	10% of quoted CAPEX cost	Successful Final Acceptance Test of all commissioned IT and Non-IT systems and Issue Go-Live Certificate from OCAC
9	Completion of one year of O&M phase	10% of quoted CAPEX cost	Satisfactory performance of the successful bidder towards the configuration, operations and incident management related to CSOC.

Payment terms regarding operations and maintenance of CSOC infrastructure (including all civil, IT and Non-IT assets)

- For the first year period, any payment towards operations and maintenance would not be made to the bidder, although any penalty towards breach of SLA for the period would be applicable to the bidder.
- The operations and maintenance cost would be initiated from the onset of the second year of operations by the bidder after Go-live.
- The SLA compliance and measurement of the services provided by the bidder would be computed by OCAC or any agency designated by OCAC.
- The OPEX would be as per the AMC and support cost for the CSOC infrastructure. The AMC and support should be for the whole duration of the bidder contract period. Any gap in the AMC or support would result in non-payment of the O&M cost proposed by the bidder.
- All payments would be done after evaluation and approval of the Payment Approval Committee (PAC) constituted by OCAC.
- All invoices should be submitted in triplicate copies.

Sr. No.	Activity	Timeline	Remarks	Payment terms
1.	Operations and maintenance cost	36 months (no payment towards O&M would be made to the successful bidder during the first year of O&M phase)	Operations and Maintenance (for IT and Non-IT items) as per the financial proposal submitted by the bidder to be distributed uniformly into 12 quarter periods.	Quarterly O&M payment = OPEX cost / 12

Payment terms regarding manpower of CSOC

All payment towards the manpower constituted for CSOC would be considered from the date all the resources are on board and in full attendance.

Sr. No.	Activity	Timeline	Remarks	Payment terms
1.	Manpower cost	48 months	The Manpower cost as per the financial proposal submitted by the bidder to be distributed uniformly into 16 quarter periods.	Quarterly Manpower payment = OPEX cost / 16

11.1 Penalty

11.1.1 Supply, Installation, Commissioning

- All the items as mentioned in the BOM should be supplied, delivered and commissioned within the mentioned timelines. Any delay would attract penalty.
- In case only some items of BOM are not as per timelines, then penalty would calculated on pro-rata basis item wise.
- The date of commissioning would be considered the date when a written communication would be sent by the bidder to OCAC for PAT readiness.
- All penalties related to supply, installation and commissioning is capped at 20% of the prescribed payment for the respective milestone.

Sr. No.	Activity	Timeline	Penalty	Remarks
1	Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval	T0 + 4 weeks	Deduction of 1% of the prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment.	On delay of more than 8 weeks, OCAC may issue a letter for improvement to the successful bidder. Failing which OCAC may proceed to terminate the contract with the successful bidder.
2	Finalization and Approval of the submitted layout, etc.	T0 + 6 weeks		
3	Completion of Structural, Architectural, Civil & Interior Works.	T0 + 16 weeks		
4	Supply, Installation and Commissioning & Testing of all Non-IT asset. Supply, Installation and Commissioning of all IT Equipment	T0 + 22 weeks	Deduction of 2% of the prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment.	On delay of more than 8 weeks, OCAC may issue a letter for informed to the successful bidder. Failing which OCAC may proceed to terminate the contract with the

Sr. No.	Activity	Timeline	Penalty	Remarks
				successful bidder.
5	Project Sign-Off & FAT (Go-Live of the Project)	T0 + 24 weeks	Deduction of 2% of the prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment.	On delay of more than 8 weeks OCAC may issue letter of termination and the work would be carried out by OCAC or any other assigned agency.
6	Submission of PBG	Within 30 days of LOI / Award to contract to successful bidder	Rs. 50,000/- per week of delay. To be measured on pro-rata day basis.	----------
7	Deployment of manpower proposed for SOC	Within 15 days of successful PAT / UAT of the SOC infrastructure.	Rs. 10,000/- per individual manpower / per week of delay. To be measured on pro-rata basis as per deployment of manpower.	----------

11.1.2 Operations and Maintenance

- All penalty should be calculated quarterly as per Quarterly Guaranteed Revenue (QGR) billed by the bidder.
- The penalty for the first year (Y1) of operations and maintenance would be deducted from the first QGR amount or would be adjusted from the 10% of CAPEX reserved for the satisfactory performance and services rendered for the first year of O&M.
- In case the incident penalty and individual parameters penalty coincides, the higher amount of penalty among the two would be considered.
- Relaxation may be provided in the first quarter period after Go-live for stabilization of the CSOC infrastructure and optimization of alerts generated.
- Overall SLA penalty amount related to operations and maintenance is capped at a maximum value of 20% of the QGR amount.

Incident Management

Sr. No.	Definition	Measurement Interval	SLA Target	Penalty terms
1.	Incident Logging	Monthly	• 100% logging of all alerts and security incidents. • 100% logging of all department / official reporting of incidents.	Rs. 5000 for every incident not logged.
2.	**Incident resolution**			
a.	**Scenario 1: When the bidder has full control and authority for the mitigation of the incident**			
(a)	Critical	Monthly	Mitigation of incident - Less than the next 3 hours	<3 hours - No penalty; >=3 hours – 1% of QGR value for every hour of delay.
			Identification and isolation of the threat or vulnerability or incident – 1 hour	More than 1 hour - 1% of QGR
(b)	High		Mitigation of incident - Less than the next 6 hours	<6 hours – no penalty; >=6 hours – 0.5% of QGR value for every hour of delay.
			Identification and isolation of the threat or vulnerability or incident - 2 hours	More than 2 hours - 1% of QGR
(c)	Medium		Mitigation of incident - Less than 3 days	<3 days – no penalty; >=3days – Rs. 10,000 for every day delay.
(d)	Low		Mitigation of incident - Less than 7 days	<7 days – no penalty; >=7 days – Rs. 5,000 for every day of delay.

Sr. No.	Definition	Measurement Interval	SLA Target	Penalty terms
ii.	**Scenario 2: When the bidder is dependent on other Stakeholders (OSDC, OSWAN, Odisha State IT centre, Other departments under CSOC) for mitigation of incident**			

Sr. No.	Definition	Measurement Interval		SLA Target	Penalty terms
(a)	Critical	Monthly	Level 3 escalation to OCAC and the concerned department / stakeholder	After 12 hours of second escalation	On failure of timely escalation, 1% of the QGR value.
			Level 2 escalation to OCAC and the concerned department / stakeholder	After 8 hours of first escalation	On failure of timely escalation, 0.5% of the QGR value.
			Level 1 escalation to OCAC and the concerned department / stakeholder.	Less than 3 hours	On failure of timely escalation, 0.25% of the QGR value.
			Identification and isolation of the threat or vulnerability or incident	1 hour	More than 1 hour - 1% of QGR
(b)	High		Level 3 escalation to OCAC and the concerned department / stakeholder	After 24 hours of second escalation	On failure of timely escalation, 1% of the QGR value.
			Level 2 escalation to OCAC and the concerned department / stakeholder	After 12 hours of first escalation	On failure of timely escalation, 0.5% of the QGR value.
			Level 1 escalation to OCAC and the concerned department / stakeholder.	Less than 6 hours	On failure of timely escalation, 0.25% of the QGR value.
			Identification and isolation of the threat or vulnerability or incident	2 hours	More than 2 hours - 1% of QGR
(c)	Medium		Level 3 escalation to OCAC and the concerned department / stakeholder	After 72 hours of second escalation	On failure of timely escalation, 0.5% of the QGR value.
			Level 2 escalation to OCAC and the concerned department / stakeholder	After 48 hours of first escalation	On failure of timely escalation, 0.25% of the QGR value.
			Level 1 escalation to OCAC and the concerned department /	Less than 48 hours	On failure of timely escalation, 0.1% of the QGR

Sr. No.	Definition	Measurement Interval		SLA Target	Penalty terms
			stakeholder.		value.
(d)	Low		Level 3 escalation to OCAC and the concerned department / stakeholder	After 07 days of second escalation	On failure of timely escalation, 0.5% of the QGR value.
			Level 2 escalation to OCAC and the concerned department / stakeholder	After 03 days of first escalation	On failure of timely escalation, 0.25% of the QGR value.
			Level 1 escalation to OCAC and the concerned department / stakeholder.	Less than 4 days	On failure of timely escalation, 0.1% of the QGR value.

Service Availability

Sl. No.	Definition	Measurement Interval	SLA Target	Penalty terms
1.	Device uptime / Device availability	Monthly	>=99.90%	>=99.90% No penalty
				>=98.00%; <99.90% 0.5% of QGR value
				>=95.00%; < 98.00% 1% of QGR value
				<95.00% 1% of QGR value for very percentage drop
2.	SOC application / software availability	Monthly	>=99.90%	>=99.90% No penalty
				>=98.00%; <99.90% 0.5% of QGR value
				>=95.00%; < 98.00% 1% of QGR value
				<95.00% 1% of QGR value for very percentage drop

Sl. No.	Definition	Measurement Interval	SLA Target	Penalty terms
3.	Manpower availability	Monthly	100% attendance as per defined in Section 9.1.3 of the RFP document.	Resource replacement with equivalent skills and experience / with approval from department – no penalty.
				Level 1 resource absent: Equal cost of the resource proposed by the bidder per day on pro rata basis.
				CSOC engineer and Level 2 resource absent: Double the cost proposed by the bidder per day on pro rata basis.
				Security Admin and Threat Intel expert and SOC Manager absent (without approval): 0.1% of QGR value.
4.	Surveillance and monitoring	Monthly	24*7*365 uptime of all CCTV cameras.	Fault in all the cameras / video recording system – Rs. 50,000 per day.
				Fault in any one of the cameras – Rs. 5000 per day / per camera.
				Fault in wiring to the camera – Rs. 5000 per day / per camera.
			60 days continuous recording of CCTV footage.	Missing footage: Rs. 5000 per hour of missing CCTV footage.
			Archival of CCTV footage for one year.	Rs. 10,000 for every instance of assessment.
5.	Business Continuity Plan testing	Yearly	A BCP drill should be conducted once a year to test the redundancy and point of failures in the SOC design.	Failure to do BCP test within the quarter period: 1% of QGR value.
				Failure to do BCP for the specific year: 1% of QGR value.
6.	Electrical power and back up			
(a)	Power DB	Monthly	Resolution to incident less than 4 hours	Power DB failure: Less than 4 hours for resolution – no penalty.
				Power DB failure: More than 4 hours 0.1% of QGR value per

Sl. No.	Definition	Measurement Interval	SLA Target	Penalty terms
				hour
				Any component faulty but DB still operative for power output: Rs. 1000 per day per component.
(b)	UPS	Monthly	Resolution to incident less than 12 hours	Both UPS faulty and no power output: Less than 12 hours - No penalty
				Both UPS faulty and no power output: More than 12 hours 1% of QGR value
				One of the two UPS faulty: Rs. 1000 per hour
				Any module of the UPS faulty (LED, display, etc.): Rs. 1000 per day
7.	Access Control	Monthly	100% operational 24*7*365	Fault in complete access control system: 0.1% of QGR value per day
				Fault in one access control unit: Rs. 5,000 per day
8.	Fire alarm	Monthly	100% operational 24*7*365	Fault in complete fire alarm system: 0.1% of QGR value per day
				Fault in one fire alarm unit: Rs. 5,000 per day
9.	Rodent repellent	Monthly	100% operational 24*7*365	Fault in complete system: Rs. 1,000 per day
				Fault in one unit: Rs. 500 per day
10.	Civil works	Monthly	100% operational 24*7*365	Any major incident: Rs. 5,000 per day
				Any minor incident: Rs. 1000 per day
11.	Electrical works	Monthly	100% operational 24*7*365	Light fault: Rs. 1000 per day per light fixture
				Any major electrical incident: Rs. 5,000 per day
				Any minor electrical incident: Rs. 1,000 per day

11.1.3 Manpower

Sr. No.	Parameter	SLA	Penalty
1	Substitution of Resources from those whose CVs provided during the technical evaluation	No substitution of resources would be allowed whose CVs / resumes had been provided with the technical bid against the RFP within 180 days from the submission of the bid (except in case of death, medical incapacity or resignation).	A penalty amount of Rs. 50,000/- would be applicable to the successful bidder per substitution per CV / resume proposed with the technical bid.
2	Replacement of resources during operations and maintenance phase	• Any replacement would not be allowed during the first year of SOC operations and maintenance (except in case of death, medical incapacity or resignation). • The replacement would be limited to SOC Engineer, Level1 and Level2 analyst only (except in case of death, medical incapacity or resignation). • The replacement resource should have similar qualification and experience as the replaced resource.	A penalty of 0.1% of the total cost of project would be applicable to the successful bidder for every replacement deviating from the SLA.

12. Reporting

- Reports to be submitted by the successful bidder are not limited to the below mentioned deliverables. The bidder has to generate and share information or reports as and when required by the client for any device, incident, service, etc.
- The report template are to be prepared by the successful bidder and shared with OCAC for review and approval.
- OCAC at any point in the duration of the contract may request the successful bidder to modify the format / data points / template of the reports.
- OCAC at any time during the contract period may request the successful bidder to share a report for any specific period for any specific parameters. The reports may be on need basis and has to be shared by the successful bidder as required.
- The scope of Vulnerability assessment would be limited to the hardware / software / applications under the scope of the successful bidder. Any other VA/PT would be on request by OCAC and on need basis.

Sr no.	Deliverable name	Deliverable timeline / frequency	Report to be shared with
1.	Weekly incident report	Weekly basis – Every Monday of consecutive week	Department SPOC / Joint GM (Tech) / PMU
2.	Monthly incident report	Monthly basis – Every second day of the consecutive month	Department SPOC / GM (Admin) / Joint GM (Tech) / PMU
3.	Availability report	Monthly basis – Every second day of the consecutive month • Availability of all the devices installed in COSC. • Availability of all the software and applications in CSOC.	Department SPOC / GM (Admin)/ Joint GM (Tech) / PMU
4.	SLA compliance report	Monthly basis – for the measurement of SLA as per the parameters mentioned in Section 14.1 of the RFP document.	Department SPOC / GM (Admin) / Joint GM (Tech) / PMU
5.	Risk report	On real time basis / request basis • When any severe incident / risk is detected or observed. • Plan for mitigating the risk. • Timelines for action against the risk observed.	Department SPOC / GM (Admin) / Joint GM (Tech)/ CEO / concerned department Head
6.	Root cause analysis report	On real time basis / request basis • When a risk is mitigated. • Details of incident. • Impact of incident. • Process of mitigation. • Steps taken for future actions.	Department SPOC / GM (Admin) / Joint GM (Tech)
7.	Vulnerability assessment report*	Quarterly basis / On real time / request basis • List of vulnerabilities observed in the system.	Department SPOC / GM (Admin) / Joint GM (Tech)

Sr no.	Deliverable name	Deliverable timeline / frequency	Report to be shared with
		• List of risks and vulnerabilities observed in the application. • Action taken against each vulnerability. • Risk details of each vulnerability. • Recommendation against each vulnerability.	
8.	Utilization report	Quarterly basis • Details of utilization device / apllication wise. • Top visited websites. • Top high utilzation devices / users. • Bandwidth utilization. • Storage details. • Physical memory utlization. • Average CPU utilization.	Department SPOC / GM (Admin)/ Joint GM (Tech) / PMU
9.	Business Continuity Plan report	Yearly basis • Testing of redundancy and point of failure in the SOC design / architecture. • Testing for service high availability, network as redundancy and devices as redundancy. • Testing of the fire alarm system, mock fire drill and access control system.	Department SPOC / GM (Admin) / Joint GM (Tech) / PMU
10.	Training report	Yearly basis • Provide training regarding technology utilized in SOC. • Provide training regarding latest and upcoming technology in SOC. • Cyber security based products and solutions training from respective OEMs. • Feedback from each attendee.	Department SPOC / GM (Admin) / Joint GM (Tech) / PMU

***Note:** Vulnerability assessment scope and period of deliverable would be established as per the stakeholder and OCAC approval and discussion.

13. Bill of Materials for CSOC

13.1 IT assets

IT assets (Indicative)		
Sr. No	**Item Description**	**QTY**
Network		
1	Management Switch - 24 port	2
2	Router	1
3	16 port PoE Switch	1
4	L2 Switch - 48 port	2
Solution		
1	Log Management appliance (Logger with Connector)*	4 / 6
2	Network Traffic analyzer	1
3	Anti – Advanced Persistent Threat Intelligence	2
4	Security Orchestration, Automation and Response (SOAR)	1
5	Security Information and Event Management (SIEM)#	0/1
6	Vulnerability Management Solution	1
7	Network Monitoring, Helpdesk & Ticketing software	1
Storage		
1	SAN Switch	2
2	SAN	1
Others		
1	Threat Intelligence feeds and updates	1
2	Training	1
Desktop / Printer		
1	Desktop	17
2	LED monitors - additional	16
3	Multifunction printer	1

Note:

*Log Management appliances should be proposed as 4 nos. in quantity if existing asset is to be upgraded and utilized and 6 nos. quantity to be proposed if new assets and solutions are to be proposed by the bidder.

SIEM should be proposed as 0 nos. (zero) in quantity if existing asset is to be upgraded and utilized and 1 nos. (One) quantity to be proposed if new asset and solution is to be proposed by the bidder.

13.2 Non-IT assets

Non – IT assets (Indicative)			
Sr. No	**Item Description**	**UOM**	**QTY**
Civil and Interiors			
1	Flooring		
a	False flooring	Sqr Mtr	Bidder to Propose
b	Italian Marble / Composite stone flooring	Sqr Mtr	Bidder to Propose
c	Carpet flooring	Sqr Mtr	Bidder to Propose
2	Partitions and Panelling	Sqr Mtr	Bidder to Propose
3	Paint	Sqr Mtr	Bidder to Propose

Non – IT assets (Indicative)			
Sr. No	**Item Description**	**UOM**	**QTY**
4	Doors		
a	Double leaf glass door	Nos	Bidder to Propose
b	Fire rated steel door	Nos	Bidder to Propose
c	Fire rated toughened glass door	Nos	Bidder to Propose
5	False ceiling	Sqr Mtr	Bidder to Propose
a	Metal Baffle ceiling	Sqr Mtr	Bidder to Propose
b	Designer Acoustic false ceiling	Sqr Mtr	Bidder to Propose
c	Curvilinear or designer ceiling	Sqr Mtr	Bidder to Propose
6	Air Conditioning	Sqr Mtr	Bidder to Propose
7	Electrical Wires, Switches & Conduits for ceiling and floor lights	Sqr Mtr	Bidder to Propose
8	Passive Cabling with components	Sqr Mtr	Bidder to Propose
9	LED Ceiling lights		
a	General LED lights	Nos	Bidder to Propose
b	Circular / Dimmable LED lights	Nos	Bidder to Propose
c	LED strips	Nos	Bidder to Propose
10	Distribution Board with Electrical MCB complete	Nos	Bidder to Propose
11	Modular switch board with switches and sockets for Desk with complete wiring	Nos	Bidder to Propose
12	Earth pit	Nos.	3
13	Perforated cable tray (factory made galvanized)	Mtr	Bidder to Propose
14	Cable raceway for cabling and wiring	Mtr	Bidder to Propose
Electrical			
1	UPS - 20 KVA	Nos	2
2	Battery bank	Set	2
Furniture			
1	Command centre control desk - 8 seater capacity	Nos	2
2	Manager Table	Nos	1
3	Meeting room table	Nos	1
4	Reception Table	Nos	1
5	Command centre chair	Nos	16
6	Chair for office and reception	Nos	6
7	Manager's chair	Nos	1
8	Storage Units	Nos	2
9	Staff Locker unit	Nos.	Bidder to Propose
10	Key Box	Nos	1
11	Dust bin (Stainless steel)	Nos	4
12	White board - Glass pasted	Nos	2
13	Sofa set	Nos	2
14	Coffee table	Nos	1
15	Pin up Notice board	Nos	2
Safety & Security System			
1	Close circuit tele vision (CCTV) NVR - 16 channel	Nos	1

Non – IT assets (Indicative)			
Sr. No	**Item Description**	**UOM**	**QTY**
2	Dome camera – IP based	Nos	9
3	32 inch Display screen	Nos	2
4	Door Access control system for 8 access controls with main panel & software	Set	1
5	Rodent repellent system	Set	1
6	Fire extinguisher - handheld	Nos	5
7	Addressable Fire Detection and Alarm system with software (20 detectors, 3 sirens)	Set	1
Network			
1	42U Rack with 48 port jack panel	Nos	1
2	LED Display (70 inch)	Nos	8
3	Video wall controller & speakers with all accessories	Set	1

13.3 Manpower requirement

Sr. No	Manpower Designation	No. of resource
1	SOC manager	1
2	Security administration and Threat Intelligence expert	1
3	SOC Engineer	3
4	SOC Level 2 Analyst	7
5	SOC Level 1 Analyst	7
6	Receptionist	1
	TOTAL	**20**

14. General conditions of contract for bidder

14.1 General terms

1. All solutions proposed by the bidder should be of latest manufacturing product and not more than 01 year old from the bid submission date, latest configuration and should not reach end of life or end of support for at least 07 years after installation.
2. All cost / price of the items quoted by the bidder would be fixed for the period of the contract and any new procurement or upgradation of the respective item would be done basis the quoted price.
3. The certifications of the manpower resources proposed for the project should be valid during the bid submission and also for the entire duration of the project. Bidder should ensure to reissue any expired certification from the relevant body.
4. All items proposed by the bidder should support dual stack, both IPV4 and IPV6 technology.
5. The bidder should ensure that the best practices of SOC are implemented during the duration of the contract.
6. All items should be under the AMC of the OEM and OEM should continue to provide support even if the bidder exits in between the agreement period.
7. All AMC, licenses, ownership, etc. of assets (hardware or software) should be in the name of OCAC.
8. All customized tools, configurations would be the property of OCAC and the bidder would have no claim whatsoever.
9. The bidder during the period of project should adhere to all the regulation and rules laid by the Government of Odisha in terms of Information Technology.
10. All IPR would be in the name of OCAC and bidder would hand over all configurations and customized tools to OCAC during exit.
11. The successful bidder shall the take the responsibility of collecting a Non-disclosure agreement signed by all the resources deployed for CSOC project and share the same with OCAC.
12. The successful bidder should implement and operate the engagement as per industry standards and security standards such ISO 27001, MeiTY, CERT-In, etc.
13. The successful bidder should submit the Performance Bank Guarantee to OCAC within 30 days of Letter of intent / Award of project contract.
14. The Performance Bank Guarantee (PBG) submitted by the successful bidder should have a validity of at least 60 days beyond the contract period.
15. Any obsolete asset would be supported for inclusion in CSOC by the prospective implementation agency, maybe subject to upgradation or technical support.
16. The proposed manpower should be deployed at SOC within 15 days of successful PAT / UAT of the complete infrastructure.
17. All Non-IT assets proposed by the bidder against the RFP should have authorized service support locally available at Bhubaneswar.
18. Any electrical / cabling rectification, repair within the CSOC premises would be the responsibility of the successful bidder and OCAC would bear no liability or borne any cost for the CSOC premises.
19. Retention of all data related to CSOC and relevant reports should be stored for minimum one year period (combining online and offline data) by the successful bidder.

20. OCAC will review the performance of the bidder against the SLA at any given time or duration of the project. The supervision report about the performance of any services pursuant to this SLA by the successful bidder or any other agency as appointed by OCAC shall form the basis for imposing damages / penalties for breach of contract. OCAC reserves the right to appoint a third-party auditor / agency to validate the deliverables under the SLA of this RFP.
21. The successful bidder during the duration of the agreement period should consult and coordinate with PMU and OCAC for expansion and integration of any additional department and stakeholder with Odisha SOC.
22. The successful bidder should consult with PMU and take approval from OCAC for any change management activities at any time of the project.
23. The successful bidder at any time of the project should cooperate with any PMU / third party agency appointed by OCAC for monitoring of SOC services and SLA compliances as and when required.

14.2 Insurance

1. Appropriate insurance to cover all solution components for the transit period and until the time of its acceptance at the respective site is to be taken by the successful bidder. As the successful bidder will carry the risk for the material in his books during transit, the successful bidder should arrange insurance for the total system as period from the dispatch till Final Acceptance Test is successfully achieved. Further the Successful bidder is to take all required insurance coverage in respect of all its personnel who shall be working on this engagement.
2. Any insurance during the operation and maintenance period of the project should be done by the successful bidder with prior acceptance form the department / OCAC.
3. The cost of insurance during the implementation is to be borne by the successful bidder and should be included in the financial proposal submitted.
4. The cost of insurance during the operation and maintenance period would be borne by OCAC on actuals, provided the insurance is done by the successful bidder only with prior acceptance from OCAC.

14.3 Confidentiality

1. OCAC may allow the implementation agency to utilize Confidential Information and the implementation agency shall maintain the highest level of secrecy, confidentiality and privacy with regard to such Confidential Information. The implementation agency shall use its best efforts to protect the confidentiality and proprietary of Confidential Information.
2. Additionally, the implementation agency shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities. The implementation agency shall use the information only to execute the Project.
3. OCAC shall retain all rights to prevent, stop and if required take the necessary punitive action against the implementation agency regarding any forbidden disclosure.
4. The implementation agency may share the confidential information with its employees, affiliates, agents and subcontractors but only strictly on a need to know basis in order to accomplish the scope of services under the Agreement.

Upon request of OCAC, the implementation agency shall execute a corporate non-disclosure agreement (NDA) with OCAC in the mutually agreed format provided by OCAC shall ensure that all its employees, agents and sub-contractors are governed by confidential obligations similar to the one contained herein. The implementation agency and its antecedents shall be bound by the NDA. The implementation agency will be held responsible for any breach of the NDA by its antecedents/ delegates/ employee/ subcontractors etc.

5. To the extent the implementation agency shares its confidential or proprietary information with OCAC for effective performance of the Services, the provisions of the confidentiality Clause (I) to (iii) shall apply mutatis mutandis on OCAC.
6. The implementation agency shall not use Confidential Information, the name or the logo of the OCAC except for the purposes of providing the Service as specified under the agreement.

14.4 Indemnification

The implementation agency hereby indemnifies, hold harmless & undertakes to defend OCAC, its affiliates and their respective employees, officers and directors against any claim by a third party including but not limited to damages, costs, expenses as a result of such claim with regard to:

- the extent that the services provided to OCAC by the implementation agency under this Agreement infringes any third party's intellectual property rights;
- taxes/charges/cess/levies (and interest or penalties assessed thereon) against OCAC that are obligations of bidder pursuant to the agreement;
- any damages for bodily injury (including death) and damage to real property and tangible personal property caused by the implementation agency;
- any claim or action by or on behalf of the implementation agency personnel based on his or her employment with the implementation agency, including claims arising under occupational health and safety, worker's compensation, provident fund or other applicable laws or regulations;
- claims by government regulators or agencies for fines, penalties, sanctions or other remedies arising from or in connection with the implementation agency's failure to comply with its regulatory/legal requirements and compliances;
- any claim on account of an alleged breach of confidentiality and security of data occurring as a result of acts of omissions or commission of the implementation agency's employees or sub-contractors;
- any claim occurring on account of misconduct, negligence or wrongful acts of omission and commission of employees of the implementation agency, and/or its sub-contractors;
- any claim occurring on account of misuse or negligent application, misuse of systems, failure to follow established procedure by the implementation agency and/or sub-contractor's employees;
- Implementation agency shall ensure compliance with all applicable laws, local and Central, including all labour laws like ESI, EPF, Minimum Wages Act, Odisha Shops & Establishments Act, Contract Labour (Regulation and abolition) Act 1970, Payment of Bonus Act etc. and shall keep First Part indemnified and harmless in case of any action for violation by Second Part of any of the applicable laws so long as this arrangement is in force. For all purposes the persons deployed will be employees of second part and they will have no relation whatsoever with First Part. Second Part shall be

responsible to furnish all such information/documents to First Part in this regard as may be required by it from time to time. Furthermore, Second part shall be responsible to furnish self- attested copies of all returns/challans filed by second part in the office of ESI, EPF, Minimum Wages Act, Contract Labour etc. on monthly basis to the first party, in case, the second part fails to submit or not willing to submit the copies of returns, first part shall be entitle to stop the payments till the submissions of the returns.

- In event of any theft, loss, damage, destruction, or any other act of vandalism or sabotage of the property of the purchaser in the possession of the bidder by virtue of the agreement, the implementation agency shall be liable to indemnify the first part to the extent of damage or loss so caused.
- Implementation agency has all the requisite consents, licenses and permissions to (I) enter into the Agreement (ii) carry out the obligations set out in the Agreement and it shall keep all such consents, licenses and permissions renewed and valid at all times during the continuance of the agreement.

14.5 Limitation of liability for implementation agency

14.5.1 The implementation agency shall be liable to the client / purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs or loss of reputation.

14.5.2 The aggregate liability of the implementation agency to the client / purchaser, whether under the contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the successful bidder to indemnify the client with respect to intellectual property rights infringement.

14.5.3 The above mentioned points **14.3.1** and **14.3.2** are applicable provided they do not exclude or limit any liabilities of either party in ways not permitted by applicable law.

14.6 Liquidated damages

If the implementation agency fails to deliver any or all of the services within the time period(s) specified in the RFP, OCAC shall without prejudice to its other remedies under agreement, deduct from the Agreement Price, as liquidated damages, a sum equivalent to, as per the SLA terms indicated in the bid document, until actual delivery or performance, subject to a maximum of 20% of the project value / project cost quoted by the bidder.

If the implementation agency requires an extension of time in completion of contractual supply on account of occurrence of any hindrance, he shall apply in writing to the authority, which has placed the supply order, for the same immediately on occurrence of the hindrance but not after the stipulated date of completion of supply. Delivery period may be extended with or without liquidated damages if the delay in the supply of equipment / software / components is on account of hindrances beyond the control of the bidder.

If OCAC fails to provide space at the respective sites of SOC and/or delay in statutory/ regulatory approvals/ non availability of bandwidth, the Liquidated damages for such delay shall not be levied on the implementation agency.

14.7 Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the implementation agency or OCAC as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:

- Neither Party shall be responsible to the other for any delay or failure in performance of its obligations due to any occurrence commonly known as Force Majeure which is beyond the control of any parties, including, but is not limited to, flood, explosion, thundering, acts of God or any Governmental body, public disorder, riots, embargoes, or strikes, acts of military authority, epidemics, lockouts or other labour disputes, insurrections, civil commotion, war, enemy actions.
- If a Force Majeure arises, the implementation agency shall notify promptly within a reasonable time frame to OCAC in writing of such condition and the cause thereof. Unless otherwise directed by OCAC, implementation agency shall continue to perform his obligations under the agreement as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
- The implementation agency shall be excused from performance of his obligations in whole or part as long as such cases, circumstances or events shall continue to prevent or delay such performance. Neither Party shall have any liability to the other Party in respect of the termination of the Agreement as a result of an event of Force Majeure.
- In case of a Force Majeure, all Parties will endeavour to agree on an alternate mode of Performance in order to ensure the continuity of service and implementation of the obligations of a party under the agreement and to minimize any adverse consequences of Force Majeure.
- Implementation agency shall be paid for supply and services till last date of termination in case of force majeure
- If force majeure conditions continue for more than 30 days and the services are suspended then either party has the right to terminate this agreement.

14.8 Intellectual Property Rights

a. All Intellectual Property of OCAC under the agreement will belong exclusively to GoO, except the pre-existing intellectual property rights of the implementation agency (if any). On payment of all fees in connection with the agreement and subject to the other provisions of the agreement, GoO shall at all times retain to use within its internal business all right title and interest in and to any Intellectual Property Rights in the deliverables to be provided by the implementation agency under the agreement and any modifications thereto or works derived from there except the pre-existing intellectual property rights of the implementation agency (if any). It is hereby expressly clarified that implementation agency shall have no

right, title or interest in or to such Intellectual Property Rights of OCAC for any purpose, except the right to use, modify, enhance and operate such designs, programs, modifications as per requirement of OCAC. Implementation agency shall not use such Intellectual Property of OCAC for any other purpose during and after the term of the Contract.

b. No services covered under the agreement shall be sold or disposed by the implementation agency to OCAC in violation of any right whatsoever of third party, and in particular, but without prejudice to the generality of the foregoing, of any patent right, trademark or similar right, or any charge mortgage or lien.
c. Subject to clause (d) below, the Intellectual Property Rights of all the database, programs, reports, formats etc. developed/created for this project would be of OCAC / GoO.
d. The implementation agency shall continue to retain sole ownership of the pre-existing proprietary knowledge, tools, source code, records, SOPs, application configurations, drawings, methodology, templates, works of authorship, materials, information plus any modifications or enhancements thereto and intellectual property content brought in by implementation agency to this engagement and/or incorporated in the deliverables submitted by bidder to OCAC or created independently of the performance of the services. For avoidance of doubt, it is clarified that the implementation agency shall have the right to use any works of authorship or other intellectual property that may be included in the deliverables, to develop for themselves, or for others, materials or processes that may be similar to those produced as a result of the services. Further, any third party licenses other than the hardware and software to be used by the implementation agency resources for delivering the deliverables under the agreement, necessary for the performance of the Services under this Agreement, would need to be procured by OCAC.
e. Implementation agency hereby undertakes; not to provide access to the Intellectual Property of OCAC to persons other than authorized users to ensure that all authorized users are appropriately notified of the importance of respecting the Intellectual Property Rights of OCAC and that they are made aware of and undertake to abide by the similar terms and conditions of the agreement. Not to permit any person, other than the authorized users, to copy, duplicate, translate into any language, or in any way reproduce the Intellectual Property of OCAC. To effect and maintain reasonable security measures to safeguard the Intellectual Property of OCAC from unauthorized access or use by any third party other than the authorized users. To notify OCAC promptly of any unauthorized disclosure, use or copying of the Intellectual Property of OCAC of which the implementation agency becomes aware. To change the manpower deployed if OCAC notifies issue (along with the justifiable ground) in the satisfactory performance of the respective resource.

14.9 Change control

OCAC may at any time during the duration of the project, with a prior written intimation given to the implementation agency make changes within the general scope and coverage of the agreement.

If any such change causes an increase or decrease in the cost of, or the time required for the implementation agency performance of any part of the work under the Agreement, whether changed or not changed by the order, an equitable adjustment shall be made in the Agreement price or delivery schedule, or both and the Agreement shall accordingly be amended, based on mutual discussions.

Implementation agency shall not charge for any cost incurred for configuration / reconfiguration of the equipment / services as directed by OCAC on account of regulatory compliance / guidelines issued by GoO and GoI.

14.10 Publicity

Any publicity by the implementation agency in which the name of OCAC is to be used, should be done only with the explicit written permission from OCAC.

14.11 Termination

14.11.1 Termination for client's convenience

- The client may at any time terminate the contract for any reason by giving the implementation agency a notice of 90 days for termination. The implementation agency shall be paid for all acceptable work done until the effective date of termination.
- Upon receipt of the notice of termination under the above point, the implementation agency shall either as soon as reasonably practical or upon the date specified in the notice of termination
    - ❖ Cease all further work, except for such work as the client may specify in the notice of termination for the sole purpose of protecting that part of the system already executed, or any work required to leave the site in a clean and safe condition;
    - ❖ Remove all implementation agency's equipment from the site, repatriate the implementation agency's personnel from the site, remove from the site any wreckage, rubbish, and debris of any kind;
    - ❖ In addition, the implementation agency, subject to the payment shall:
        - Deliver to the client the parts of the system / project executed by the implementation agency up to the date of termination;
        - To the extent legally possible, assign to the client all right, title, and benefit of the implementation agency to the system, or subsystem, as at the date of termination, and as may be required by the client;
        - Deliver to the client all non-proprietary drawings, specifications, and other documents prepared by the bidder as of the date of termination in connection with the system.

14.11.2 Termination for implementation agency's default

14.11.2.1 The client, without prejudice to any other rights or remedies it may possess, may terminate the agreement forthwith in the following circumstances by giving a notice of 30 days for termination and its reasons therefore to the implementation agency:

a. If the implementation agency becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the implementation agency is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the implementation agency takes or suffers any other analogous action in consequence of debt;
b. If the implementation agency assigns or transfers the contract or any right or interest therein in violation of the provision of contract; or
c. If the implementation agency, in the judgment of the client, has engaged in corrupt or fraudulent practices in competing for or in executing the contract, including but not limited to wilful misrepresentation of facts concerning ownership of intellectual property rights in, or proper authorization and/or licenses from the owner to offer, the hardware, software, or materials provided under agreement / contract.

   For the purposes of this Clause:
   "Corrupt practice" means the offering, giving, receiving, or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution.

   "Fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the client and includes collusive practices among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the client of the benefits of free and open competition.

   "Unfair trade practices" means supply of goods (hardware, networking equipment, etc.) different from what is mentioned in the bid documents, and includes change of parts/ components, use of refurbished / repaired / sub-standard / duplicate parts instead of genuine new parts or change the specifications and/or make of the company for which the supply order was given by client.

14.11.2.2 If the implementation agency:

a. Has abandoned or repudiated the Contract;
b. Has without valid reason failed to commence work on the project / system promptly;

c. Persistently fails to execute the Contract in accordance with the Contract or persistently neglects to carry out its obligations under the Contract without just cause;
d. Refuses or is unable to provide sufficient Materials, Services, or labour to execute and complete the System in the manner specified in the agreed project plan furnished under the RFP / contract at rates of progress that give reasonable assurance to the client that the implementation agency can attain operational acceptance of the system by the time for achieving operational acceptance as extended; then the client may, without prejudice to any other rights it may possess under the agreement, give a notice to the implementation agency stating the nature of the default and requiring the implementation agency to remedy the same. If the implementation agency fails to remedy or to take steps to remedy the same within 30 days of its receipt of such notice, then the client may terminate the agreement forthwith by giving a notice of termination to the implementation agency.

Upon receipt of the notice of termination under the above point, the implementation agency shall either as soon as reasonably practical or upon the date specified in the notice of termination

a. Cease all further work, except for such work as the client may specify in the notice of termination for the sole purpose of protecting that part of the system already executed, or any work required to leave the site in a clean and safe condition;
b. Remove all implementation agency's equipment from the site, repatriate the implementation agency's personnel from the site, remove from the site any wreckage, rubbish, and debris of any kind;
c. In addition, the implementation agency, subject to the payment shall:
    i. Deliver to the client the parts of the system / project executed by the bidder up to the date of termination;
    ii. To the extent legally possible, assign to the client all right, title, and benefit of the implementation agency to the system, or subsystem, as at the date of termination, and as may be required by the client;
    iii. Deliver to the client all non-proprietary drawings, specifications, and other documents prepared by the implementation agency as of the date of termination in connection with the system.

14.11.3 General terms during termination

- The client may enter upon the site, expel the implementation agency, and complete the system itself or by employing any third party. Upon completion of the system or at such earlier date as the client thinks appropriate, the client shall give notice to the implementation agency that such implementation agency's equipment will be returned to the bidder at or near the site and shall return such implementation agency's equipment to the implementation agency in accordance with such notice. The implementation agency shall thereafter without delay and at its cost remove or arrange removal of the same from the site.

- If there are any sum due on implementation agency, the client shall deduct the same accruing prior to the date of termination from the amount to be paid to the bidder under the agreement.

- If the client completes the system, the cost of completing the system by the client shall be determined. If the sum that the implementation agency is entitled to be paid, plus the reasonable costs incurred by the client in completing the system, exceeds the Agreement Price, the implementation agency shall be liable for such excess, limited to the total cost of the project as submitted by the implementation agency. If such excess is greater than the sums due the implementation agency, the implementation agency shall pay the balance to the client, and if such excess is less than the sums due the implementation agency, the client shall pay the balance to the implementation agency. The client and the implementation agency shall agree, in writing, on the computation described above and the manner in which any sums shall be paid.

- The Performance Bank Guarantee shall be invoked in case of termination under termination by implementation agency or termination by implementation agency's default.

14.12 Taxes and Duties

All payments will be subjected to tax deduction at source as applicable/ required at the prevailing tax rates. Any changes, revision or enactment in duties like GST, taxes or any CESS during the period of validity of the bids and also during the agreement period by Central/State/Other Government bodies will be considered and applied after due consideration. The decision of OCAC in this regard will be final and binding and no dispute will be entertain. Any taxes at the time of supply goods and services shall be applicable as per the Law.

For goods supplied from outside the Purchaser's country, the bidder shall be entirely responsible for all applicable taxes, license fees, and other such levies imposed outside the Purchaser's country. The basic price quoted item wise by the bidder in respect of the transaction between OCAC & the bidder shall include all taxes & duties and charges payable by the bidder except for the GST, CGST plus OGST, or IGST, as the case may be, at applicable rate shall be quoted alongside the basic price for all the items. However, while quoting the basic price against the package/works, benefit of Input Tax Credit (ITC) should be adjusted in the quoted price by the bidder.

14.13 Settlement of Disputes

- OCAC and the implementation agency shall make every effort to resolve amicably by direct informal negotiation, any disagreement or dispute, arising between them under or in connection with the contract.
- In case of any doubts about a clause of the contract agreement which includes contract documents, the interpretation given by the client shall be final and binding, till the time any other interpretation is ordered in the case by arbitration tribunal.

- If any dispute of any kind whatsoever shall arise between the client and the implementation agency in connection with or arising out of the agreement, including without prejudice to the generality of the foregoing, any question regarding its existence, validity, or termination, or the operation of the System (whether during the progress of implementation or after its achieving Operational Acceptance and whether before or after the termination, abandonment, or breach of the agreement), the parties shall seek to resolve any such dispute or difference by mutual consultation. If the parties fail to resolve such a dispute or difference by mutual consultation within 60 days, upon expiry of which either party may move to the notification of arbitration.
- In case of any dispute between the client and the implementation agency arising out of the breach or noncompliance of any condition of the Contract, the dispute shall be resolved in accordance with the provisions of the Arbitration and Conciliation Act, 1996 (No. 26 of 1996).
- All arbitration proceedings would be held only under the legal jurisdiction of Bhubaneswar or Cuttack.

15. Obligations of OCAC

1. OCAC would coordinate and assist in acquiring all permissions required for civil construction, earth pit, area for outdoor installations, cooling system, power connectivity from OCAC Tower, back-up power connectivity from OCAC tower.
2. Cooling cost, Bandwidth cost, Diesel Cost (if required) and Electricity Cost will be borne by OCAC and this cost is not part of the scope of the bidder. OCAC shall directly engage with these service providers and pay them directly.
3. Physical security costs of the CSOC would be borne by OCAC and recruitment of physical security guards would be done by OCAC.
4. Critical devices like CSOC servers, CSOC appliances and CSOC network devices would be installed at the State Data Centre.
5. Power supply, network connectivity, rack space, cooling, internet bandwidth to the above mentioned critical devices would be provided by Odisha SDC.
6. Housekeeping and general up-keep (example: sweeping, dusting, etc.) of CSOC would be the responsibility of OCAC.

16. Exit Management

The successful bidder shall not exit from the agreement within stipulated time period of four (4) years after Go-Live. However, in the event that the successful bidder decides to opt out of the contract prematurely it has to notify the authority six months in advance through a written letter, the successful bidder will not seek ownership rights over the equipment and PBG will also be forfeited.

16.1 Purpose

- This section sets out the provisions which will apply upon completion of the agreement period or upon termination of the agreement for any reasons.
- Both parties shall ensure that their respective associated entities, in case of OCAC, any third party appointed by the OCAC and in case of the successful bidder, the

OEMs or another OEM authorized partner, carry out their respective obligations during exit period.

- The exit management period starts, in case of expiry of agreement, on the date when the agreement comes to an end or in case of termination of agreement, on the date when the notice of termination is sent to the successful bidder.
- The exit management period ends in three months after the beginning of the exit management period.

16.2 Exit management period

During the exit management period, the successful bidder shall ensure that:

- All project assets including the hardware, software, documentation and any other infrastructure shall have been cured of all defects and deficiencies as necessary so that the assets are compliant with the specifications and standards set forth by OCAC.
- The successful bidder shall deliver relevant records and reports pertaining to the CSOC Project and its design, engineering, operation, and maintenance including all operation and maintenance records and manuals pertaining thereto and complete to OCAC before end of exit period.
- The Successful bidder shall comply with all other requirements as may be prescribed under Applicable Laws to complete the exit management and assignment of all the rights, title and interest of the successful bidder in the CSOC project free from all encumbrances absolutely and free of any charge or tax to OCAC or its nominee.
- The successful bidder will allow OCAC or any third party appointed by OCAC, access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable OCAC or any third party appointed by OCAC to assess the existing services being delivered.
- The successful bidder during the period of exit would share every artefact related but not limited to:
    I. Documentation of customized tools or software.
    II. User manuals and SOPs for various process and operations.
    III. Documentation related to support and AMC.
    IV. Licenses and ownership documents.
    V. Previous reports including all status reports.

16.3 Exit management plan

The successful bidder should prepare an exit management plan and share the same with OCAC within 90 days of signing of agreement. The EMP should contain:

- A detailed program of the transfer process that could be used in conjunction with OCAC or any third party appointed by OCAC including details of the means to be used to ensure continuing provision of the services throughout the transfer process and of the management structure to be used during the transfer.
- Plans for the communication with OCAC and any related third party as are necessary to avoid any material detrimental impact on OCAC's operations as a result of undertaking the transfer.
- Identification and implementation of specific tasks necessary during the exit period.

- Timelines of activities to be done by OCAC and the successful bidders during the exit management period.

The exit management plan has to be updated whenever necessary and shared with OCAC annually every year.

Annexure – I: Current asset detail

Odisha State Data Centre (OSDC)

Details of servers installed at the Odisha State Data Centre (OSDC)

Sr. No	Asset Name	Asset Description	Make	Model	Quantity
1	SERVER	HYPER-V SERVER	IBM	BL-HS22	1
2	SERVER	ADDITIONAL DOMAIN CONTROLLER SERVER	IBM	BL-HS22	1
3	SERVER	HYPER-V SERVER	IBM	BL-HS22	1
4	SERVER	PROXY SERVER	IBM	BL-HS22	1
5	SERVER	HYPER-V SERVER	IBM	BL-HS22	6
6	SERVER	DATABASE SERVER ON AIX PLATFORM	IBM	P-550	3
7	SERVER	DATABASE SERVER ON WINDOWS PLATFORM	IBM	X-3850 M2	2
8	SERVER	TIVOLI STORAGE MANAGEMENT SERVER	IBM	X-3850 M2	1
9	SERVER	STAGGING SERVER	IBM	X-3850 M2	1
10	SERVER	CA TIM SERVER	IBM	X-3850 M2	1
11	SERVER	ORACLE RAC SERVER	IBM	P-550	1
12	SERVER	APPLICATION SERVER ON WINDOWS PLATFORM	IBM	BL-HS22	1
13	SERVER	NETWORK FAULT MANAGEMENT SERVER	IBM	BL-HS22	1
14	SERVER	NETWORK PERFORMANCE MANAGEMENT SERVER	IBM	BL-HS22	1
15	SERVER	HELPDESK SERVER	IBM	BL-HS22	1
16	SERVER	SERVER MANAGEMENT SERVER	IBM	BL-HS22	1
17	SERVER	DATABASE MANAGEMENT SERVER	IBM	BL-HS22	1
18	SERVER	ORACLE RAC SERVER	IBM	P-550	1
19	SERVER	WEB APPLICATION SERVER ON WINDOWS PLATFORM	IBM	BL-HS22	1
20	SERVER	WEB APPLICATION SERVER ON WINDOWS PLATFORM	IBM	BL-HS22	1
21	BLADE CHASIS	IBM BLADE CHASIS	IBM	MT 8677	1
22	BLADE CHASIS	IBM BLADE CHASIS	IBM	MT 8677	1
23	SERVER	HYPER-V SERVER	IBM	BL-HS23	4
24	SERVER	HYPER-V SERVER	HP	BL460C G9	8
25	BLADE CHASIS	HP BLADE CHASIS	HP	BLC 7000C	1
26	SERVER	Esxi Server	HP	HPEDL380	12
27	SERVER	Esxi Server	DELL	DELL EMC POWER EDGE R740	12

Details of ESM solution installed at the Odisha State Data Centre (OSDC)

Sr. no.	Solution name	Product version	OEM	Model	Installed Server Make and model	Quantity
1.	Enterprise Security Manager (ESM)	6.9	ArcSight	Flexconnect - 10000 EPS licensed	HP DL380 Gen9	1
2.	Logger	6.4	ArcSight	L7600 OS: Redhat Enterprise Linux (Maipo)	HP DL380 Gen9	2
3.	Connector	2.8	ArcSight	C6600 OS: Redhat Enterprise Linux (Maipo)	HP DL380 Gen9	2
4.	User Behaviour Analyser	5.2	ArcSight	Basic 1K Actor	HP DL380 Gen9	1

Note: The support for the above solution expires in December 2021.

Details of storage devices installed at the Odisha State Data Centre (OSDC)

Sr. No.	Asset Name	Asset Manufacturer	Make / Model	Quantity
1	SAN Switch	CISCO	DS-C9134-K9	4
2	Storage	IBM	DS 5300	1
3	Storage Disk Self	IBM	EXP 5000	14
4	VTL Disk self	IBM	TS 7520	12
5	VTL Base server	IBM	TS 7500 SERVER	2
6	Tape Library	IBM	IBM LT04 UDS3	2
7	Hitachi VSP Replicator	HITACHI	HJ-4230-7EWEA	1
8	Brocade Switch	Brocade	Brocade 7800	2
9	MDS/SAN Switch	Cisco	DSC9148-32P-K9	2
10	SAN STORAGE	DELL	SC 7020	1
11	NAS	DELL	FS 8600	1
12	SAN Switch	HPE	HPSN6500B	2
13	SAN STORAGE	HPE	HPE 3 PAR 8440	1
14	Storage Disk Self	HPE	HPE 3 PAR 8000	8
15	StoreServ SPS Service Processor	HPE	HPE ProLiantDL120 Gen9	1
16	HPE STORE ONCE ENCLOSURE	HPE	HPE StoreOnce Enclosure (5250)	1
17	HPE STORE ONCE BASE SYSTEM	HPE	HPE StoreOnce Base System (5250)	1

Details of network devices installed at the Odisha State Data Centre (OSDC)

Sr. No.	Asset Name	Asset Manufacturer	Make / Model	Quantity
1	INTERNET ROUTER	CISCO	CISCO3845	2
2	INTERNET SWITCH	CISCO	Cat3560G-24TS	2
3	NETWORK LOADBALANCER	RADWARE	LinkProof On Demand Switch 2	2

Sr. No.	Asset Name	Asset Manufacturer	Make / Model	Quantity
4	IPS	RADWARE	DP-1016-NL-D-Q	2
5	INTERNET FIREWALL	CISCO	Cisco ASA5580	2
6	CORE SWITCH	CISCO	WS-C6509-E	2
7	WEB DMZ SWITCH	CISCO	Cat3560G-24TS	2
8	APP LOADBALANCER	RADWARE	AppDirector with Cookie Persistency	2
9	INTRANET FIREWALL	CISCO	Cisco ASA5550	2
10	MGM DMZ SWITCH	CISCO	Cat3560G-24TS	2
11	APP & DB DMZ SWITCH	CISCO	Cat3560G-24TS	2
12	ACCESS SWITCH	CISCO	Cat3560G-24TS	1
13	Access Control Server (AAA Server)	CISCO	Cisco 1120 Secure ACS	2
14	MAIL SECURITY APPLIANCE	SYMANTEC	SYMANTEC MAIL SECURITY 8340 APPLIANCE	2
15	KVM Switch	IBM	IBM 17353LX	3
16	INTERNET FIREWALL	CISCO	Cisco FPR-C9300	1
17	FMC	CISCO	CISCO FIREPOWER MANAGEMENT CENTRE 2500	1
18	NEXUS SWITCH	CISCO	CISCO NEXUS N9K-C93180YC-FX	4
19	INTERNET FIREWALL	CISCO	Cisco FPR-C9300	1
20	IPS	RADWARE	RADWARE Defence Pro	2
21	APP LOADBALANCER	RADWARE	RADWARE ALTEON 6029	2
22	VPN	CISCO	Cisco ASA5525-X	2

Details of peripherals installed at the Odisha State Data Centre (OSDC)

Sr. No.	Asset Name	Asset Manufacturer	Make / Model	Quantity
1	Desktop	DELL	OPTIPLEX 380	10
11	Desktop	HP	HP COMPAQ DX2480	1
12	Desktop	DELL	OPTIPLEX 9010	6
18	Laptop	Dell	VOSTRO 1015	6
23	Laptop	Dell	VOSTRO 3460	4
27	Laptop	Dell	LATITUDE E5510	1
29	Laptop	Dell	INSPIRON N5050	1
30	Laptop	Dell	INSPIRON 15	2
32	Laptop	ACER	Gateway 4250s	1

Details of applications hosted in Odisha State Data Centre (OSDC)

Sr. No.	Application Name	User Department	Mode of Hosting
1	BETAN	Electronics & Information Technology	Shared
2	Odisha Mail	Electronics & Information Technology	Shared
3	Odisha Online	Electronics & Information	Shared

Sr. No.	Application Name	User Department	Mode of Hosting
	(Citizen centric e-Services like payment of electricity bill, water bill, online application for birth & Death certificate etc.)	Technology	
4	Social Media Grievance Management	Electronics & Information Technology	Shared
5	SRDH (State Residence Data Hub) SRDH_Authentication SRDH_eKYC	Electronics & Information Technology	Co-Located
6	e-District	Electronics & Information Technology	Co-Located
7	Portal of OESL (Odisha e-Governance Service Ltd.)	Electronics & Information Technology	C0-Located
8	Odisha.gov.in	Electronics & Information Technology	Shared
9	SANJOG	Electronics & Information Technology	Shared
10	OCAC.IN	Electronics & Information Technology	Shared
11	MO SARKAR	Electronics & Information Technology	Shared
12	Resident Commissioner Portal	Home	Shared
13	OSSC (Odisha Staff Selection Commission)	General Administration & Public Grievance	Shared
14	OSSC-Online	General Administration & Public Grievance	Shared
15	MAMATA (Web MIS of Scheme for Pregnant Women)	Women & Child Development & Mission Shakti	Shared
16	Shakti Varta	Women & Child Development & Mission Shakti	Shared
17	e-Pragati	Women & Child Development & Mission Shakti	Shared
18	WCD website	Women & Child Development & Mission Shakti	Shared
19	WPMS (Works Project Monitoring & Payment Solution System)	ST & SC Development, Minorities & Backward Classes Welfare	Shared
20	dcodisha online	Health & Family Welfare	Shared
21	RHCLMIS	Health & Family Welfare	Shared
22	State DBT (World Bank) Web Portal	Finance	Shared
23	ODRP (MIS Application of OSDMA)	Revenue & Disaster Management	Shared
24	PAIS (Property Allotment Information System, BDA)	Housing & Urban Development	Shared
25	BBSROne	Housing & Urban Development	Shared
26	STA_OMVD	Commerce & Transport	Shared
27	STA_Portal	Commerce & Transport	Shared

Sr. No.	Application Name	User Department	Mode of Hosting
28	STARTUP ODISHA	Micro, Small & Medium Enterprise	Shared
29	Claimant Management System	Higher Education Department	Shared
30	RTS Odisha (OREDA)	Science & Technology	Shared
31	Invest Odisha_IPICOL	Industries	Shared
32	Shri Jagannath Temple Inquiry commission	Law	Shared
33	OPSC (Odisha Public Service Commission)	General Administration & Public Grievance	C0-Located
34	OPSC online	General Administration & Public Grievance	C0-Located
35	WAMIS (Works & Account Management Information System)	Rural Development	C0-Located
36	i3MS (integrated Mines & Minerals Management System)	Steel & Mines	C0-Located
37	e-Bitaran	Food Supplies & Consumer Welfare	C0-Located
38	ERP Application_SAP	Food Supplies & Consumer Welfare	C0-Located
39	P-PAS (Paddy Procurement Automation System)	Food Supplies & Consumer Welfare	C0-Located
40	SCMS (Supply Chain Management System)	Food Supplies & Consumer Welfare	C0-Located
41	MDM Application_IBM	Food Supplies & Consumer Welfare	C0-Located
42	PIMS (Personnel Information Management System)	Food Supplies & Consumer Welfare	C0-Located
43	FPS Automation (Fair Price Shops Automation)	Food Supplies & Consumer Welfare	C0-Located
44	Food Odisha Portal & Website	Food Supplies & Consumer Welfare	C0-Located
45	Grievance Redressal System	Food Supplies & Consumer Welfare	C0-Located
46	BKKY (Biju Krushak Kalayan Yojana)	Agriculture & Farmers' Empowerment	C0-Located
47	krushipanipaga	Agriculture & Farmers' Empowerment	Co-Located
48	IVR _Advisory Solution for farmers	Agriculture & Farmers' Empowerment	Co-Located
49	ORSAC (Orsac new website)	Science & Technology	C0-Located
50	ORSAC (Kenduleaves Orissa)	Science & Technology	C0-Located
51	ORSAC (Banking-Network-Odisha)	Science & Technology	C0-Located
52	ORSAC	Science & Technology	C0-Located

Sr. No.	Application Name	User Department	Mode of Hosting
	(Web GIS System for IPICOL/IDCO)		
53	ORSAC (Stage Carriage Permit Management System_STA)	Science & Technology	C0-Located
54	ORSAC (Web Application VTS (Vehicle Tracking System)_I3MS)	Science & Technology	C0-Located
55	CTD (Commercial Tax Department)	Finance	C0-Located
56	IFMS (Integrated Financial Management System)	Finance	C0-Located
57	OPHWC (ERP application of Odisha Police Housing Welfare Corporation)	Home	C0-Located
58	CCTNS_SCRB (Crime and Criminal Tracking Network & Systems)	Home	Co-Located
59	e-Registration	Revenue & Disaster Management	Co-Located
60	NMMP (BMC_PMC)	Housing & Urban Development	Co-Located
61	e-Municipality	Housing & Urban Development	Co-Located
62	Pension Odisha	Finance	shared
63	Skill Odisha	Skill Development & Technical Education	shared
64	CTD (Commercial Tax Department)	Finance	C0-Located
65	Web Portal of Directorate of Ports and Inland Water Transport	Commerce & Transport	shared
66	Social Security & Empowerment of Persons with Disabilities (SSEPD)	Social Security & Empowerment of Persons with Disabilities	shared
67	e-Niramaya / Odisha State Medical Corporation Limited (OSMC)	Health & Family Welfare	Shared
68	Odia Phalaka	Labour & Employees' State Insurance	Shared
69	Sishu Suchana	Women & Child Development & Mission Shakti	Shared
70	Odia Virtual Academy	Odia Language Literature & Culture Department	Shared
71	Bijuli Batti	Energy	Shared
72	ADAPT	Agriculture & Farmers' Empowerment	Shared
73	Make in Odisha (MIO)_IPICOL	Industries	Shared
74	TDCC (Tribal development co-operative corp.)	ST & SC Development, Minorities & Backward Classes Welfare	Co-located
75	TDCC_MPAS	ST & SC Development, Minorities & Backward Classes Welfare	Co-located

Sr. No.	Application Name	User Department	Mode of Hosting
76	Odisha Primary Education Programme Authority (OPEPA)	School & Mass Education	Co-located
77	Contractor Database Management System (CDMS)	Works	Shared
78	DLM	Food Supplies & Consumer Welfare	Co-located
79	BIJUYUVA	Sports & Youth Services	Shared
80	HOCKEYODISHA	Sports & Youth Services	Shared
81	RAJBHAVAN	Home	Shared
82	KALIA	Agriculture & Farmers' Empowerment	Shared
83	Bank Aggregator System	Agriculture & Farmers' Empowerment	Shared
84	ORERA (Odisha Real Estate Regulatory Authority)	Housing & Urban Development	Shared
85	AAHAAR	Housing & Urban Development	Shared
86	AWAAS / OUHM (Odisha Urban Housing Mission)	Housing & Urban Development	Shared
87	e-SUSHRUT/e-Swasthya/OeHIMS	Health & Family Welfare	Shared
88	e-Swachh Odisha	Housing & Urban Development	Shared
89	EXCISE	Excise	Shared
90	Biju Swastya Kalyan Yojana (BSKY)	Health & Family Welfare	Shared
91	Shri Jagannath Temple Administration	Law	Shared
92	Odisha School Education Programme Authority (OSEPA) MIS APP	School & Mass Education	Shared
93	Odisha School Education Programme Authority (OSEPA) WEB	School & Mass Education	Shared
94	Odisha School Education Programme Authority (OSEPA) SMA APP	School & Mass Education	Shared
95	Odisha School Education Programme Authority (OSEPA) PMA APP	School & Mass Education	Shared
96	Odisha Youth Innovation Fund	Micro, Small & Medium Enterprise	Shared
97	Integrated Legal Monitoring System (ILMS)	School & Mass Education	Shared
98	Tubewell Management system (TMS)	Panchayati Raj and Drinking Water	Shared
99	e-prashikyan	Women & Child Development & Mission Shakti	Shared
100	RTDAS	Forest & Environment	Shared
101	SSEPD Scheme	Social Security & Empowerment of Persons with Disabilities	Shared
102	Rural Development Website	Rural Development	Shared
103	Administration of Incentive Module (AIM)	Micro, Small & Medium Enterprise	Shared
104	Revenue Minister's Helpline	Revenue & Disaster Management	Shared
105	KRUTI Application	Handlooms, Textiles & Handicrafts	Shared

Sr. No.	Application Name	User Department	Mode of Hosting
106	Website of Pathanisamanta Planetarium	Science & Technology	Shared
107	Website of Directorate of Higher Education	Higher Education Department	Shared
108	MOPRIDE	Housing & Urban Development	Shared
109	Air Quality Index (AQI) Mobile App	Forest & Environment	Shared
110	GEET	Panchayati Raj and Drinking Water	Shared
111	eAbkari	Excise	Shared
112	Feedback Management System	Food Supplies & Consumer Welfare	Shared
113	MIS RTE Pardarshi	School & Mass Education	Shared
114	MO SARKAR_H&UD	Housing & Urban Development	Shared
115	MO SCHOOL	School & Mass Education	Shared
116	Odisha Sanitation	Panchayati Raj and Drinking Water	Shared
117	OMBADC	Planning & Convergence	Shared
118	MO SARKAR_SSEPD	Social Security & Empowerment of Persons with Disabilities	Shared
119	Swachha Odisha Sustha Odisha (SOSO)	Panchayati Raj and Drinking Water	Shared

Details of email solution installed at the Odisha State Data Centre (OSDC)

Sr. No.	Description	Details
1	**Name and version of the mail messaging solution / suite**	Postfix SMTP (version 2.10.1), Cyrus IMAP (version 1.00), Apache (version 2.4.6), PHP (version 5.4.16)
2	**Solution Installation**	In virtual environment
3	**Operating system on which the email messaging system is installed**	CentOS
4	**Number of users utilizing or enlisted for the email service currently**	148
5	**Directory service utilized**	LDAP

State IT centre

Details of devices installed at State IT Centre

Sr. No.	Description Of Asset	Make	Model	Quantity
1	Core Switch	Cisco	Nexus N9K-C9508	2
2	Core Switch	HPE	12904E	2
3	Distribution Switch	Cisco	Nexus C92160YC-X	9
		HPE	5940	7
4	ASA	Cisco	ASA 5540	1
5	ASA	Cisco	ASA 5510	1
6	Firewall	Checkpoint	122000	2
7	Content Analyser	Forcepoint	V10000 G4	2
8	Content Management solution	Forcepoint	Smart-1210	1
9	Load Balancer	RADWARE	Alteon NG-6024(VX)	2
10	Load balancer management solution	RADWARE	APSolute Vision	1
11	Router	Cisco	Cisco-2811	1
12	Router	Cisco	Cisco7200	1
13	Wireless Controller	Aruba	Aruba 6000	2
14		Aruba	Aruba 7205	2
15		Cisco	AIRWLC2106-K9	2
16	Switches	CISCO	SGE2000P	65
17	Switches	CISCO	2960X	159
18	Switches	CISCO	C3560	1
19	Switches	HP	A5120	12
20			A5500	1
21			1620	1
22	Wireless access point	Aruba	AP305	61
23			AP93	150
24	Blade Server	HP	HPEProLiant BL 460C GEN9	6
25	Production Server	HP	HPE ProLiant DL 380 GEN9	5
26	SAN Switch	HP	HP SN6010C	2
27	Access Switch	HP	HP 5130 - 24G - 4SFP	2
28	Server Load Balancer	Array Networks	APV 2600	2
29	Tape Library	HP	HPE MSL4048	1
30	Production Server	HP	HPE ProLiant DL 380 GEN9	3
31	Access Switch	HP	HPE 5130 -24G-4SFP	1
32	Software Firewall	HP	ProLiant DL180 G5	1
33	SMS Gateway	IBM	System x3650	1
34	Application	IBM	System x3650	1
35	Application Backup	IBM	System x3650	1
36	Database-sql	IBM	x3850	1
37	Application Backup	HP	ProLiant DL580 G5	1

Sr. No.	Description Of Asset	Make	Model	Quantity
38	Application	HP	ProLiant DL180 G5	1
39	Website	HP	ProLiant DL180 G5	1
40	Website	IBM	System x3650	1
41	Database-sql	IBM	System x3650	1
42	web application	HP	ProLiant DL580 G7	1
43	Software Firewall	Lenovo	--------	1
44	Storage	HP	--------	3
45	Application	HP	ProLiant DL180 G6	1
46	Database-sql	HP	ProLiant DL180 G6	1
47	Cluster Database	HP Blade	ProLiant BL420c Gen8	1
48	Cluster Database	HP Blade	ProLiant BL420c Gen8	1
49	Wagios, PObsitagios, PO	HP Blade	ProLiant BL420c Gen8	1
50	Westing(Cbsitesting(C	HP Blade	ProLiant BL420c Gen8	1
51	Application	HP Blade	ProLiant BL420c Gen8	1
52	Website	HP Blade	ProLiant BL420c Gen8	1
53	Application	HP Blade	ProLiant BL420c Gen8	1
54	Application	HP Blade	ProLiant BL420c Gen8	1
55	AD-DNS	HP Blade	ProLiant BL420c Gen8	1
56	Website	HP Blade	ProLiant BL420c Gen8	1
57	Antivirus	HP Blade	ProLiant BL420c Gen8	1
58	Application	HP Blade	ProLiant BL420c Gen8	1
59	Application	HP Blade	ProLiant BL460c Gen10	5
60	SQL Server 2017 Cluster	HP Blade	ProLiant BL460c Gen10	2

Details of application hosted at State IT Centre

Sr. No.	Web Portal / Application	Department
1	Odisha Secretariat Workflow Automation System (OSWAS)	E&IT
2	Student Academic Management System (SAMS)	E&IT

State Wide Area Network (SWAN)

Details of devices at State Headquarters

Sr. No.	Equipment Details	Make	Model	Quantity
1	Core Router	Cisco	ASR-1013X	1
2	Switch	Cisco	4510	1
3	Switch	Cisco	3500	1
4	Switch	Cisco	CE-500	1
5	Switch	HP	HPE-5940	1
6	Firewall & IPS	Checkpoint	23500	2
7	Web-Security	Forcepoint	V10KG4	2
8	Antivirus Server	Quick Heal	SEQRITE	1
9	AAA Server	HP	Clear Pass-2000	2
10	RMX	Polycom	RMX 2000	2
11	DMA	Polycom	DMA 7000	2
12	Resource Manager	Polycom	Resource Manager	2

Details of devices at District Headquarters

Sr. No.	Equipment Detail	Make	Model	Quantity
1	Router	Cisco	ASR 1001X	30
2	Switch	Cisco	3560	30

Details of devices at Block Headquarters

Sr. No.	Equipment Detail	Make	Model	Quantity
1	Router	Cisco	ISR4300	200
2	Router	Cisco	ISR2911	84
3	Switch	Cisco	CE-500	209
4	Switch	Cisco	WS-2960	75

Assets which are obsolete or approaching obsolescence:

State Data Centre (SDC)

Sl. No.	Asset name	Make/Model	Quantity	EOS date
1	Router	Cisco 3845	2	October 31, 2016
2	Access Switch	Cisco 3560G-24TS	9	January 31, 2018
3	Internet Firewall	Cisco ASA5580	2	July 31, 2017
4	Intranet Firewall	Cisco ASA5550	2	September 30, 2018
5	Access Control Server	Cisco 1120 Secure	2	May 31, 2016

Sl. No.	Asset name	Make/Model	Quantity	EOS date
	(AAA)	ACS		

State Wide Area Network (SWAN)

Sl. No.	Asset name	Make/Model	Quantity
1	Core Switch	Cisco 4510	1
2	LAN switch	Cisco 3550	2
3	DDOS	Radware 3200	1
4	L2 Switch – DHQ	Cisco 3560	15
5	L2 Switch – BHQ	Cisco CE 500	208

Events per second generated by the devices at SDC, SWAN and State IT centre:

Events per second for the existing infrastructure under current scope of work

Sr. No.	Measurement	No. of devices	Value
1	Estimated events per second for average 24 hours	1342	8000
2	Estimated events per second during peak hours	1342	21000

Additional events per second for the proposed additional infrastructure during expansion of CSOC under extended scope of work

Sr. No.	Measurement	No. of devices	Value
1	Estimated events per second for average 24 hours	381	5200
2	Estimated events per second during peak hours	381	14000

Note:

1. The successful bidder has to provide devices / infrastructure as per the current scope of work and maintain feasibility for scalability and expansion as per the extended infrastructure in future.

Annexure – II: Proforma

Proforma 1: Bidder profile

(To be declared in the bidder's letter head)

Name of the Firm/Company		
Full Address of the company		
Year Established		
Telephone Number		
Fax Number		
E-mail Address		
Website		
Sectors' in which the company / firm has provided services to Government / Departments in		
No. of full time personnel currently under employment	Level 1 analyst: Level 2 analyst: SME level:	
No. of years of presence in India		
Annual Turnover	Financial Year	Turn Over (₹)
	2016-17	
	2017-18	
	2018-19	
Authorized Representative	Name	
	Designation	
	Mobile	
	Office	
	E-mail	

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Proforma 2: Letter of Authority

(To be declared in bidder's letter head)

Date:…….

To,
The General Manager, OCAC,
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Subject: Letter of authority for RFP for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC), tender no……..

Sir,

I/We ……..hereby authorize following representative(s) to attend Pre Bid Meeting, Technical Bid opening, Financial Bid opening and for any other correspondence and communication against above Bid.

1. Name:
   Designation:
   Signature

2. Name
   Designation:
   Signature

I/We confirm that I/we shall be bound by all commitments made by aforementioned authorized representatives.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Note: The Power of attorney for authorized signatory of this document on behalf of the company should be attached with the letter.

Proforma 3: Letter for agreement to scope of work

Date:…….

To,
The General Manager (Admin),
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Subject: Submission of letter for agreement of scope of work for bidder against RFP no…….. for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC)

Sir,

We, the undersigned, have read and examined in detail the RFP documents for "Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC)".

We are in consensus to abide by the scope of work as mentioned in Section 4 of the RFP document and would provide the best of services to fulfil the scope.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Proforma 4: Undertaking on Total Responsibility

(To be declared in the bidder's letter head)

Date:…….

To,
The General Manager (Admin),
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Dear Sir,

Subject: Undertaking on Total Responsibility for Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Odisha Cyber Security Operations Centre at OCAC, Bhubaneswar.

This is to certify that we undertake total responsibility for the successful and defect free operation of the proposed Project, as per the requirements and terms and condition of the RFP for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre at OCAC, Bhubaneswar"

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Proforma 5: Forwarding Letter for Earnest Money Deposit

(To be declared in the bidder's letter head)

Forwarding Letter for Earnest Money Deposit

From (Name & complete address of the bidder) _____ _____ _____ _____	To General Manager (Admin) Odisha Computer Application Centre, N1/ 7D, Acharya Vihar Square, Near Planetarium, P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Dear Sir/Madam,

Subject: EMD submission for the RFP "Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre at OCAC, Bhubaneswar"

Reference: RFP number </_____/__> dated <__/_____/_____>

We, M/s <_____>, having carefully read and examined in detail the RFP document for "Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre" at OCAC, Bhubaneswar, published by OCAC hereby submit EMD of Rs. < _____ >/- (Rupees <_____> Only) in the form of Bank Guarantee. The details are as under:

Name of Issuing Bank :
Bank Guarantee number :
Amount :
Dated :

We M/s _____ have read and understood the clauses of RFP document towards forfeiture of EMD.

Thanking you,
Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:
Designation: Date:

Encl: - Copy of Earnest Money Deposit

Proforma 6: Format of Earnest Money Deposit (EMD)

In consideration to the advertisement published by OCAC (hereinafter called the "Purchaser") has their offer dated_____ through RFP for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre at OCAC, Bhubaneswar hereinafter called the "IA") against the purchaser's RFP enquiry No. _____/_____/_____ KNOW ALL MEN by these presents that We _____< Bank Name> of _____ having our registered office at _____ are bound unto _____ (hereinafter called the "Purchaser) in the sum of _____ for which payment will 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 ___ day of _____ , 2020.

THE CONDITIONS OF THIS OBLIGATION ARE:

(1) If the IA withdraws or amends, impairs or derogates from the RFP in any respect within the period of validity of this RFP.

(2) If the IA having been notified of the acceptance of his RFP by the purchaser during the period of its validity:-

a. If the bidder fails to furnish the Performance Security for the due performance of the contract.

b. Fails or refuses to accept/execute the contract.

We undertake to pay 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 the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including 180 days from the last date of RFP bid submission date and any demand in respect thereof should reach the Bank not later than the above date.

_____

(Signature of the authorized officer of the Bank)

_____

Name and designation of the officer

_____

Seal, name & address of the Bank and address of the Branch

Proforma 7: Compliance of Eligibility criteria

(To be declared in the bidder's letter head)

Date:…….

To,
The General Manager (Admin),
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Subject: Bidder's compliance for the eligibility criteria as per the RFP for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC) at OCAC, Bhubaneswar.

Sir,

In reference to the subject cited, please find below the details of the compliance as per the eligibility criteria mentioned in the RFP document:

Sr. No.	Pre-qualification criteria	Document to be submitted	Compliance (Yes/ No)
1	A bidder with solutions developed in an entity incorporated in a country sharing a land boundary with India cannot participate in this bid.	Declaration by the bidder / OEM on their letter head that the bidder has proposed no such solutions in response to the RFP.	
2	The bidder should be an established Company registered under the – Indian Companies Act, 1956/2013, or partnership firm register under LLP Act, 2008 since last 5 years as on 31st March 2019.	• Certificate of incorporation. • Certificate consequent to change of name if applicable.	
3	The bidder should have a registered number of: • GST Registration. • Income Tax / PAN.	• Certificate of GST registration. • Copy of PAN / Income tax number.	
4	The bidder may be either an OEM / an authorized partner of the OEM whose product bidder is proposing. (The solution proposed can be from a single or various OEMs).	In case of an OEM authorized partner, a letter of authorization (MAF) from original manufacturer for each solution / equipment must be furnished in original duly signed. Undertaking from the OEM mentioning a clause that OEM will provide support services during the complete period of	

Sr. No.	Pre-qualification criteria	Document to be submitted	Compliance (Yes/ No)
		the contract if the bidder authorized by them fails to perform.	
5	The bidder should have a minimum average annual turnover of at least Rs. 200 Crores in the last three financial years (i.e. 2016-17, 2017-18 & 2018-19).	Audited Balance Sheets for last 3 years, i.e., 2016-17, 2017-18 & 2018-19 where financial turnover is segregated. Every sheet should be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 3 financial years. **or** A letter under the head of the chartered accountant / or firm certifying the financial turnover of the company is to be submitted with the bid.	
6	The bidder should have positive net worth during the last three financial years (i.e. 2016-17, 2017-18 & 2018-19).	Audited Balance Sheets for last 3 years, i.e., 2016-17, 2017-18 & 2018-19 where profit or loss from similar works is segregated. Every sheet should be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 3 financial years. **or** A letter under the head of the chartered accountant / or firm certifying the profit and loss of the company from similar line of service is to be submitted with the bid.	
7	The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.12.2019. SOC solution could be On-premises SOC, Managed SOC, Hybrid SOC. At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5 crore.	Relevant MSA copy / Work order copy / client satisfactory letter regarding successful implementation or ongoing of security operation centre (SOC) solution in the name of the bidder is to be submitted. The PO / letter should be in the name of the bidder and clearly mention the scope of work.	

Sr. No.	Pre-qualification criteria	Document to be submitted	Compliance (Yes/ No)
8	The bidder should have local office in Odisha or should submit a declaration for establishing an office in Odisha within one month of issuing of Letter of Intent (LoI) from OCAC.	Self-certification with office location addresses to be submitted / declaration for establishment of an office in case LoI has been awarded. The document should be on the bidder's letter head signed by the authorized signatory.	
9	The bidder should not have been blacklisted by Government of India / Government of Odisha during the last three years.	An undertaking to this effect in the company's letter head signed by authorized signatory to be submitted as per Proforma 21 of the RFP document.	
10	The bidder should have minimum manpower strength as per the different skill levels defined in the document: Level 1 analyst – minimum 20. Level 2 analyst – minimum 20. SME level - minimum 3. (The manpower criteria as mentioned in the Section 8.2 and 8.3 of the RFP document) All manpower should be on the pay role of the company / bidder.	An undertaking in the company's letter head signed by authorized signatory to be submitted.	
11	The bidder should be: • ISO 9001:2008 or later certified • ISO 20000: 2018 certified • ISO 27001: 2013 certified	Copy of certificate to be submitted.	

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Proforma 8: Undertaking of Service Level Compliance

(To be declared in the bidder's letter head)

Date:……

To,
The General Manager (Admin),
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Dear Sir/Madam,

Subject: Undertaking on Service Level Compliance

1. I/We as Implementing Agency do hereby undertake that we shall monitor, maintain, and comply with the service levels stated in the RFP to provide quality service to OCAC.
2. However, if the proposed resources, Non-IT Infrastructure and ICT components are found to be insufficient in meeting the RFP and/or the service level requirements given by OCAC, then we will augment the same without any additional cost to OCAC.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Proforma 9: Warranty Certificate

(To be declared in the bidder's letter head)

Date:……..

To,
The General Manager (Admin),
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Sir/Madam,

We warrant that the equipment(s) supplied under the contract would be newly manufactured, free from all encumbrances, defects and faults in material or workmanship or manufacture, shall be of the highest grade and quality, shall be consistent with the established and generally accepted standards for materials of the type ordered, shall be in full conformity with the specifications, drawings of samples, if any, and shall operate as designed. We shall be fully responsible for its efficient and effective operation. We also warrant that the services provided under the contract shall be as per the Service Level Agreement (SLA) with Government of Odisha / OCAC.

There are no technical deviations (null deviations) from the requirement specifications of tendered items and schedule of requirements. The entire work shall be performed as per your specifications and documents. In case, any item of hardware or software is found non-compliant at any stage during project implementation, it would be replaced with a fully compliant product/solution at no additional cost to OCAC. In case of non-adherence of this activity, OCAC reserves the right to cancel the contract, in case the said contract is awarded to us by OCAC. We further certify that our proposed solution meets, is equivalent or better than the minimum technical specifications as given in the RFP.

The obligations under the warranty expressed above shall include all costs relating to labour, spares, maintenance (preventive as well as unscheduled), and transport charges from site to manufacturer's works / service facilities and back for repair or modification or replacement at site of the equipment or any part of the equipment, which under normal care and proper use and maintenance proves defective in design, material or workmanship or fails to operate effectively and efficiently or conform to the specifications and for which notice is promptly given by OCAC to us (bidder). We shall provide on-site support for all the equipment and services supplied hereunder during the period of this warranty (4 years from the date of go-live) and entire service period for services.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:
Designation: Date:

Proforma 10: Authorization letters from all OEMs

Date:…….

To,
The General Manager (Admin),
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Reference: Supply of equipment/software/License for the project "Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC) at OCAC, Bhubaneswar"

Sir/Madam,

We _____, (name and address of the manufacturer) who are established and reputed manufacturers of _____ having factories at _____ (addresses of manufacturing locations) do hereby authorize M/s _____ (name and address of the Bidder) to bid, negotiate and conclude the contract with you against the above mentioned RFP for the above equipment manufactured by us.

We also do hereby assure that we would support our equipment/software/license and freely upgrade them for a period of four years of Operations and Maintenance, from the date of go-live of the project, by M/s _____ (name and address of the Bidder) who has proposed to use for the project "Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC) at OCAC, Bhubaneswar" or his successor. We would also adhere to the timelines for maintenance as indicated in this RFP by closely working with the Bidder or his successor for a period of five years from the date of supply of the equipment. We abide by the commercials quoted by the Bidder towards AMC charges for four years from the date of supply and successful commissioning of equipment(s) i.e. Go-Live.

We confirm that the products quoted will not be end of life for next five years from the last date of submission of bids.

Yours faithfully,

For and on behalf of M/s _____ (Name of the manufacturer)

Signature _____

Name :

Designation :

Address :

Date :

Seal

Note: This letter of authority should be on the letterhead of the concerned manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.

Proforma 11: Proposal Covering Letter – Technical

(To be declared in the bidder letter head)

Date:……

To,
The General Manager (Admin),
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Subject: Submission of technical proposal against RFP no…….. for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC)

Sir,
We, the undersigned, offer to provide services to OCAC on Odisha Cyber Security Operations Centre (CSOC) with your Request for Proposal dated…….

We are hereby submitting our Proposal, which includes this Technical bid as per the Proforma, eligibility criteria and other relevant terms and conditions of the RFP.
We hereby declare that all the information and statements made in this Technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification. We agree to abide by all the terms and conditions of the RFP document. We would hold the terms of our bid valid for 180 days as stipulated in the RFP document.
We hereby declare that we are not insolvent, in receivership, bankrupt or being wound up, our affairs are not being administered by a court or a judicial officer, our business activities have not been suspended and we are not the subject of legal proceedings for any of the foregoing.

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

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Proforma 12: Compliance of Technical specification for IT and Non-IT assets

(To be declared in the bidder's letter head)

Date:……

To,
The General Manager (Admin),
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Subject: Bidder's compliance for the technical specification as per the RFP for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC)

Sir,

In reference to the subject cited, we provide assurance that all the equipment in terms of IT and Non-IT assets to be provided for the Odisha Security Operation Centre project are of the same or higher than the specifications as mentioned in the RFP - Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC) document.

In case of any discrepancy or non – compliance if observed in future; we shall be held liable for the same.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Proforma 13: Project Credentials Format

Sl. No.	Item	Detail
General Information		
1.	Customer Name/ Government Department	
2.	Details of Contact Person • Name: • Designation: • Email: • Phone: & Fax: • Mailing Address:	
Project Details		
3.	Name of the project	
4.	Government/Non-government	
5.	Start Date/End Date	
6.	Current Status	(work in Progress (PAT/FAT/Go-Live) OR completed)
7.	Contract Tenure	
8.	Area of the Data Centre	
9.	Effort involved in Payroll person-months in the complete project	
10	Order Value of the project (in Crores)	
11.	Please provide copies of Work Order or Certificate of Completion for completed projects from the customer	
More than one same table content may be provided for more than one project detail. A copy of the work order / MSA / contract should be attached with the format.		

I do hereby acknowledge that the details provided above are true to best of my knowledge.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name: Place:
Designation: Date:

Proforma 14: Format for providing CV of Manpower to be proposed

Curriculum Vitae of Key Personnel's

The bidder shall provide the summary table of details of the manpower that will be deployed on this project during the implementation.

Table-A

Sr. No	Manpower Designation	Name of resource	Highest qualification and certifications	Years of relevant experience
1	SOC manager			
2	Security administration and Threat Intelligence expert			
3	SOC Engineer			
4	SOC Level 2 Analyst			
5	SOC Level 1 Analyst			

Table-B

Sl. No.	Particulars	Details	Supporting document
1.	Key resource / Non Key resource		
2.	Name of the Personal		
3.	Current Designation/Job title		
4.	Current job responsibilities		
5.	Proposed Role in this project		
6.	Total experience and relevant experience (in years)		
7.	Number of years with the organization and date of joining the firm		
8.	Whether resource is engaged by the firm in its own payrolls	YES/NO	
9.	Summary of Professional / Domain Experience		
10.	Date of Birth		
11.	Academic Qualifications: • Degree • Academic institution graduated		Attach certificate of highest qualification

Sl. No.	Particulars	Details	Supporting document
	from • Year of graduation • Specialization (if any) • Key achievements and other relevant information (if any)		
12.	Professional Certifications/ Training		Attach relevant certificates
13.	Membership of Professional Associations		
14.	Employment Record*		
15.	• Details of similar project handled & the role assigned • Prior project experience • Project name • Customer • Key project features in brief • Location of the project • Designation • Role • Responsibilities and activities • Duration of the project		
16.	Detailed tasks Proposed to be assigned	Work already undertaken that best illustrates capability to handle the tasks assigned**	
17.	Signature of the representative		

I hereby declare that the above mentioned resource would be available during the project phase of this RFP.

*Starting with present position, list in reverse order every employment held by the staff member since graduation

**Among the assignments in which the staff has been involved, indicate brief details of the project in which this responsibility was assigned (including nature and duration of duty)

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name: Place:

Designation: Date:

Proforma 15: Proposal Covering Letter – Financial

(To be declared in the bidder letter head)

Date:……

To,
The General Manager, OCAC,
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Subject: Submission of Commercial proposal for RFP no…… for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC)

Sir,

We, the undersigned, have read and examined in detail the RFP documents for "Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC)". I / we do hereby propose to provide services as specified in the RFP document no……./…..dated …/…/……

1. Price proposal and validity

All the prices mentioned in our RFP are in accordance with the terms as specified in the RFP documents. All the prices and other terms and conditions of this RFP are valid for a period of 180 days as desired in the RFP.

We hereby confirm that our RFP prices include all taxes. However, all the taxes are quoted separately under relevant sections. We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other corporate Tax in altercated under the law, we shall pay the same.

2. Unit rates

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

3. Deviations

We declare that all the services shall be performed strictly in accordance with the RFP documents except for the variations and deviations, all of which have been detailed out exhaustively in the following statement, irrespective of whatever has been stated to the contrary anywhere else in our proposal. Further, we agree that additional conditions, if any, found in the RFP documents, other than those stated in deviation schedule, shall not be given effect to.

4. RFP pricing

We further confirm that the prices stated in our proposal are in accordance you're your Proforma included in RFP documents.

5. Qualifying data

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

6. Performance bank guarantee bond

We hereby declare that in case the contract is awarded to us, we shall submit the PBG bond in the form prescribed in Proforma of Bank Guarantee towards PBG and as per General Conditions of Contract. We hereby declare that our RFP is made in good faith, without collusion or fraud and the information contained in the RFP is true and correct to the best of our knowledge and belief. We understand that our RFP is binding on us and that you are not bound to accept any bid document you receive. We confirm that no Technical deviations are attached here with this commercial offer.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Proforma 16: Financial Proposal – IT and Non-IT (CAPEX)

(To be declared in bidder's letter head)

Sr. No	Item Description	UoM	QTY	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E =D%*C	F = C+E
IT assets (Indicative)										
Network										
1	Management Switch - 24 port	Nos.	2							
2	Network Router	Nos.	1							
3	16 port PoE Switch	Nos.	1							
4	L2 Switch - 48 port	Nos.	2							
Solution										
1	Log Management appliances (Logger with Connector)*	Nos.	4 / 6							
2	Network Traffic analyzer	Nos.	1							
3	Anti – Advanced Persistent Threat Intelligence	Nos.	2							
4	Security Orchestration, Automation and Response (SOAR)	Nos.	1							
5	Security Information and Event Management (SIEM)#	Nos.	0/1							
6	Vulnerability Management Solution	Nos.	1							
7	Network Monitoring, Helpdesk & Ticketing software	Nos.	1							
Storage										
1	SAN Switch	Nos.	2							
2	SAN	Nos.	1							

Sr. No	Item Description	UoM	QTY	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E =D%*C	F = C+E
Others										
1	Threat Intelligence feeds and updates	Nos.	1							
2	Training	Nos.	1							
Desktop / Printer										
1	Desktop	Nos.	17							
2	LED monitors - additional	Nos.	16							
3	Multifunction printer	Nos.	1							
Non – IT assets (Indicative)										
Civil and Interiors										
1	Flooring									
a	False flooring	Sqr Mtr	Bidder to Propose							
b	Italian Marble / Composite stone flooring	Sqr Mtr	Bidder to Propose							
c	Carpet flooring	Sqr Mtr	Bidder to Propose							
2	Partitions and Panelling	Sqr Mtr	Bidder to Propose							
3	Paint	Sqr Mtr	Bidder to Propose							
4	Doors									

Sr. No	Item Description	UoM	QTY	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E =D%*C	F = C+E
a	Double leaf glass door	Nos.	Bidder to Propose							
b	Fire rated steel door	Nos.	Bidder to Propose							
c	Fire rated toughened glass door	Nos.	Bidder to Propose							
5	False ceiling	Sqr Mtr	Bidder to Propose							
a	Metal Baffle ceiling	Sqr Mtr	Bidder to Propose							
b	Designer Acoustic false ceiling	Sqr Mtr	Bidder to Propose							
c	Curvilinear or designer ceiling	Sqr Mtr	Bidder to Propose							
6	Air Conditioning	Sqr Mtr	Bidder to Propose							
7	Electrical Wires, Switches & Conduits for ceiling and floor lights	Sqr Mtr	Bidder to Propose							
8	Passive Cabling with components	Sqr Mtr	Bidder to							

Sr. No	Item Description	UoM	QTY	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E =D%*C	F = C+E
			Propose							
9	LED Ceiling lights									
a	General LED lights	Nos.	Bidder to Propose							
b	Circular / Dimmable LED lights	Nos.	Bidder to Propose							
c	LED strips	Nos.	Bidder to Propose							
10	Distribution Board with Electrical MCB complete	Nos.	Bidder to Propose							
11	Modular switch board with switches and sockets for Desk with complete wiring	Nos.	Bidder to Propose							
12	Earth pit	Nos.	3							
13	Perforated cable tray (factory made galvanized)	Mtr	Bidder to Propose							
14	Cable raceway for cabling and wiring	Mtr	Bidder to Propose							
Electrical										
1	UPS - 20 KVA	Nos	2							
2	Battery bank	Set	2							

Sr. No	Item Description	UoM	QTY	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E =D%*C	F = C+E
Furniture										
1	Command centre control desk - 8 seater capacity	Nos.	2							
2	Manager Table	Nos.	1							
3	Meeting room table	Nos.	1							
4	Reception Table	Nos.	1							
5	Command centre chair	Nos.	16							
6	Chair for office and reception	Nos.	6							
7	Manager's chair	Nos.	1							
8	Storage Units	Nos.	2							
9	Staff Locker unit	Nos.	Bidder to Propose							
10	Key Box	Nos.	1							
11	Dust bin (Stainless steel)	Nos.	4							
12	White board - Glass pasted	Nos.	2							
13	Sofa set	Nos.	2							
14	Coffee table	Nos.	1							
15	Pin up Notice board	Nos.	2							
Safety & Security System										
1	Close circuit tele vision (CCTV) NVR - 16 channel	Nos.	1							
2	Dome camera – IP based	Nos.	9							
3	32 inch Display screen	Nos.	2							
4	Door Access control system for 8 access controls with main panel & software	Set	1							

Sr. No	Item Description	UoM	QTY	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E =D%*C	F = C+E
5	Rodent repellant system	Set	1							
6	Fire extinguisher - handheld	Nos.	5							
7	Adressable Fire Detection and Alarm system with software (20 detectors, 3 sirens)	Set	1							
Network										
1	42U Rack with 48 port jack panel	Nos.	1							
2	LED Display (70 inch)	Nos.	8							
3	Video wall controller & speakers with all accessories	Set	1							
Total amount (sum of all values in column C, E and F)										
Total CAPEX cost (sum of all values in column F)										
Total CAPEX cost in words (sum of all values in column F)										

Note:

* Log Management appliances should be proposed as 4 nos. in quantity if existing asset is to be upgraded and utilized and 6 nos. quantity to be proposed if new assets and solutions are to be proposed by the bidder.

SIEM should be proposed as 0 nos. (zero) in quantity if existing asset is to be upgraded and utilized and 1 nos. (One) quantity to be proposed if new asset and solution is to be proposed by the bidder.

Proforma 17: Financial Proposal – Manpower

(To be declared in bidder's letter head)

Sr. No	Manpower Designation	No. of resource	Unit price per month (in Rs.)	Total number of months	Total Price (in Rs.)	Tax rate (%)	Total tax amount (in Rs.)	Total price including tax (in Rs.)
			A	B	C = A*B	D	E=D%*C	F=C+E
1	SOC manager	1		48				
2	Security administration and Threat Intelligence expert	1		48				
3	SOC Engineer	3		48				
4	SOC Level 2 Analyst	7		48				
5	SOC Level 1 Analyst	7		48				
6	Receptionist	1		48				
Total amount (sum of all values in column C, E and F)								
Total amount in words (sum of all values in column F)								

Proforma 18: Financial Proposal – Operations and Maintenance (OPEX)

(To be declared in bidder's letter head)

Sl. No	Item Description	Year 1	Year 2	Year 3	Year 4
		OPEX (in Rs.)	OPEX (in Rs.)	OPEX (in Rs.)	OPEX (in Rs.)
		A	B	C	D
1.	Operations and Maintenance Cost estimate for IT asset	**0.00**			
2.	Operations and Maintenance Cost estimate for Non-IT asset	**0.00**			
3.	Cost estimate for proposed Manpower				
TOTAL					
Total OPEX cost (sum of total of columns A, B, C, D)					
Total OPEX cost (in words)					

Proforma 19: Financial Proposal – Total cost of the project (CAPEX + OPEX)

Sl. No	Item Description	Amount quoted by the bidder (in Rs.)
1.	Total CAPEX Cost as per Proforma 16	
2.	Total OPEX Cost as per Proforma 18	
	Grand Total	
	Grand Total (in words)	

Proforma 20: Financial Proposal – Additional cost

Any additional resource or tools if proposed by the bidder should be added as per the Proforma provided below. The bidder may add rows to the format / template if required. This proforma for additional cost will not be a part of the financial evaluation.

Additional Manpower (temporary if required on request from OCAC)

Sl. No	Manpower description	No. of resource	Unit price per month (in Rs.)	Total number of months	Total Price (in Rs.)	Tax rate (%)	Total tax amount (in Rs.)	Total price including tax (in Rs.)
			A	B	C = A*B	D	E=D%*C	F=C+E
1	Forensic Analyst	1		1				
2	Threat Hunting Specialist	1		1				
3	Security trainer	1		1				
			TOTAL					
			TOTAL (in words)					

Additional licensing / tools

Sl. No	Manpower description	Quantity / Capacity	Make & Model	Unit price (in Rs.)	Total Price (in Rs.)	Tax rate (%)	Total tax amount (in Rs.)	Total price including tax (in Rs.)
		A		B	C=A*B	D	E=D%*C	F=C+E
1	Vulnerability management solution license – per device / per IP							
2	User licenses (to be added by bidder) – per device / per user							
3	Storage per 01 TB in SAN							
4	***Any other solution to be proposed by the bidder can be mentioned by adding rows to the table****							
				TOTAL				
				TOTAL (in words)				

***Note:** The bidder has to submit the technical specification with justification for the additional solution / appliance proposed.

Proforma 21: Letter for self-declaration of clean track record

(To be declared in the bidder letter head)

To,
The General Manager, OCAC,
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Subject: Self-declaration for clean track record of services

Sir,

I hereby declare that my company……. has not been debarred / blacklisted by Government of India / Government of Odisha in the last three years for indulging in corrupt or fraudulent practices or for indulging in unfair trade practices and not backed out from executing the work after award of the work as on the RFP submission date.
My company…… is also not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this RFP.

I further certify that I am competent authority in my company has authorized me to make this declaration.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name: Place:

Designation: Date:

Proforma 22: Format of Bank guarantee

(Should be a legal document)

Ref. No._____

Bank Guarantee No _____ Dated_____

To,
The General Manager, OCAC,
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar 751013

Dear Sir,

In consideration of Odisha Computer Application Centre, Bhubaneswar, India (hereinafter referred to as 'OCAC', which expression shall, unless repugnant to the context or meaning thereof, include all its successors, administrators, executors and assignees) after receipt of the Letter of Intent (LOI) dated…… with M/s …… having it's registered / head office at …….. (hereinafter referred to as the implementation agency) which expression shall, unless repugnant to the context or meaning thereof include all its successors, administrators, executors and assignees) and OCAC having agreed that the Implementation agency shall furnish to OCAC a performance guarantee for 10% of the Total Project Cost for the faithful performance of the entire contract.

We (name of the bank) ……. registered under the laws of _____ having head / registered office at……..(hereinafter referred to as "the Bank", which expression shall, unless repugnant to the context or meaning thereof, include all its successors, administrators, executors and permitted assignees) do hereby guarantee and undertake to pay immediately on first demand in writing any / all moneys to the extent of 10% of the Total Project Cost without any demur, reservation, contest or protest and / or without any reference to the Implementation agency. Any such demand made by OCAC on the Bank by serving a written notice shall be conclusive and binding, without any proof, on the bank as regards the amount due and payable, notwithstanding any dispute(s) pending before any Court, Tribunal, Arbitrator or any other authority and / or any other matter or thing whatsoever, as liability under these presents being absolute and unequivocal. We agree that the guarantee herein contained shall be irrevocable and shall continue to be enforceable until it is discharged by OCAC in writing. This guarantee shall not be determined, discharged or affected by the liquidation, winding up, dissolution or insolvency of the implementation agency and shall remain valid, binding and operative

against the bank.

The Bank also agrees that OCAC at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor, in the first instance, without proceeding against the implementation agency and notwithstanding any security or other guarantee that OCAC may have in relation to the implementation agency's liabilities.

The Bank further agrees that OCAC shall have the fullest liberty without our consented without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by the said implementation agency from time to time or to postpone for any time or from time to time exercise of any of the powers vested in OCAC against the said implementation agency and to forbear or enforce any of the terms and conditions relating to the said agreement and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said implementation agency or for any forbearance, act or omission on the part of OCAC or any indulgence by OCAC to the said implementation agency or any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

The Bank further agrees that the Guarantee herein contained shall remain in full force during the period that is taken for the performance of the contract and all dues of OCAC under or by virtue of this contract have been fully paid and its claim satisfied or discharged or till OCAC discharges this guarantee in writing, whichever is earlier.

This Guarantee shall not be discharged by any change in our constitution, in the constitution of OCAC or that of the implementation agency.

The Bank confirms that this guarantee has been issued with observance of appropriate laws of the country of issue.

The Bank also agrees that this guarantee shall be governed and construed in accordance with Indian Laws and subject to the exclusive jurisdiction of Indian Courts of OCAC.

Notwithstanding anything contained herein above, our liability under this Guarantee is limited to Indian Rs. (in figures)……. (Indian Rupees (in words) _____) and our guarantee shall remain in force until …… (indicate OCAC date of expiry of bank guarantee). Any claim under this Guarantee must be received by us before the expiry of this Bank Guarantee. If no such claim has been received by us by the said date, the rights of OCAC

under this Guarantee will cease. However, if such a claim has been received by us within the said date, all the rights of OCAC under this Guarantee shall be valid and shall not cease until we have satisfied that claim.

In witness whereof, the Bank through its authorized officer has set its hand and stamp on this ……Day of…….……..20…. at ……

Proforma 23: Non-Disclosure Agreement

Non-Disclosure Agreement

I, <name>, aged about……<age>., employed with ……,<organization name> ("the Organization") ……..<location of office / organization) as a…… <position> in the …… <service line> have been deputed/assigned to work on ……<project name> ("the Engagement") for Organization's client …….. <client name> ("the Client").

2. I acknowledge that as per the terms of my employment and the Code of Ethics applicable to me, I am obliged to keep all confidential information of the Organization, its affiliates or associates, including but not limited to their personnel, clients, vendors, customers, business associates etc., in strictest confidence and not disclose the same to anyone without the prior written consent of the Organization.

3. I acknowledge that in the course of working on the Engagement, I may have access to or become privy to or otherwise receive non-public information of or relating to the Client, its subsidiaries, affiliates or associates including but not limited to information relating to their employees, clients, vendors, customers, business associates etc. ("Confidential Information").

4. Without prejudice to the generality of my acknowledgement and obligation under paragraph 2 above, I specifically acknowledge and agree to maintain the Confidential Information in strictest confidence and not give access to, share with or otherwise disclose the same to any persons (including the Client's and Organization's personnel) other than those with whom I am required to share the Confidential Information strictly on a 'need to know' basis in the course of performing my duties under the Engagement i.e. where there is a legal or professional right to know.

5. I shall take all necessary precautions to maintain the confidentiality of the Confidential Information, including, but not limited to ensuring that:

   - All physical media that holds Confidential Information (i.e., papers, CD-ROMs, tapes, envelops, binders, file folders, etc.) are always stored in secure places when not in use.
   - My computer system is always locked with password when left unattended.
   - Confidential Information pertaining to the Engagement is deleted from my laptop after archiving all necessary information, data and files in accordance with the archival policies.

6. I agree that my obligation to maintain the confidentiality of the Confidential Information shall survive and continue to apply even after the termination of the Engagement and my employment with the Organization

Signature:

Dated:

Proforma 24: Undertaking on Exit Management

(To be declared in the bidder letter head)

Date:……..

To
General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Dear Sir/Madam,

Subject: Undertaking on Exit Management and Transition

1. I/We hereby undertake that at the time of completion of our engagement with OCAC, either at the End of Contract or termination of Contract before planned Contract Period for any reason, we shall successfully carry out the exit management and transition of this Project to OCAC or to an agency identified by OCAC to the satisfaction of OCAC. I/We further undertake to complete the following as part of the Exit management and transition:

    a. We undertake to complete the updating of all Project documents and other artefacts and handover the same to OCAC before transition.

    b. We undertake to design standard operating procedures to manage system (including application and IT systems), document the same and train OCAC personnel on the same.

    c. If OCAC decides to take over the operations and maintenance of the Project on its own or identifies or selects any other agency for providing operations & maintenance services on this Project, then we shall provide necessary handholding and transition support, which shall include but not be limited to, conducting detailed walkthrough and demonstrations for the IT Infrastructure, handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the ICT components , conducting Training sessions etc.

2. I/We also understand that the Exit management and transition will be considered complete on the basis of approval from OCAC.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name: Place:

Designation: Date

----------End of Document----------