Request for Proposal

Request for Proposal (RFP) for Selection of Agency for Supply, Installation & Commissioning of Enterprise Security Solution for Cyber Security Operation Centre (CSOC)

Government of Odisha

RFP No- OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024

Odisha **C**omputer **A**pplication **C**entre
(Technical Directorate of E & I.T. Department, Government of Odisha)
N-1/7-D, Acharya Vihar, P.O. - RRL,
Bhubaneswar - 751013
EPBX: 674-2567280 / 2567064 /2567295 / 2567283
Fax: +91-674-2567842
E-mail ID: contact@ocac.in
Website: www.ocac.in

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.

Definitions /Acronyms

Term	Definition
Agreement	Agreement to be signed between the successful bidder and OCAC, including all attachments, appendices, all documents incorporated by reference thereto together with any subsequent modifications, the RFP, the bid offer, the acceptance and all related correspondences, clarifications, presentations.
Authorized Representative	Any person authorized by either of the parties
Bidder	Any Firm/OEM offering the solution(s), service(s) and /or materials as required in the RFP. The word Bidder when used in the pre-award period shall be synonymous with parties bidding for this RFP, and when used after award of the contract shall mean the successful party with whom OCAC, signs the agreement for rendering of services for implementation of this project.
OEM	Original Equipment Manufacturer
Party	Means OCAC or Bidder, individually and “Parties” mean OCAC and Bidder, collectively
Proposal/Bid	The Pre-Qualification – cum – Technical Proposal and Commercial Proposals all together, i.e., complete proposal for the implementation of this project
Request for Proposal (RFP)	Means this document and its annexure etc., seeking a set of solution(s), services(s), materials and/or any combination of them.
PBG	Performance Bank Guarantee
CSOC	Cyber Security Operation Centre
OCAC	Odisha Computer Application Centre

RFP SCHEDULE

Sl. No.	Items	Date & Time
1.	Availability of Bid Document in the website (www.ocac.in, www.odisha.gov.in & www.enivida.odisha.gov.in)	01-March-2024
2.	Last date for receiving queries through e-mail: gm_ocac@ocac.in & csoc@odisha.gov.in	06-March-2024 by 05:00 PM
3.	Pre-bid Conference	12-March-2024 at 12:30 PM
4.	Issue of Corrigendum (If any)	15-March-2024
5.	Last date and time for Submission of Bid through www.enivida.odisha.gov.in	30-March-2024 by 02:00 PM
6.	Opening of Pre-Qualification (PQ) – cum-Technical Bid for Package - I	30-March-2024 at 04:00 PM
7.	Opening of Pre-Qualification (PQ) Bid for Package-II	30-March-2024 at 04:00 PM
8.	Opening of Technical Qualification (TQ)Bid for Package -II	To be Intimated Later
9.	Date of Technical Presentation for Package - II	To be Intimated Later
10.	Opening of Commercial Bids for Package – I & Package - II	To be Intimated Later

Table of Contents

1. Fact Sheet

<table>
<tr><th>Clause Reference</th><th>Topic</th></tr>
<tr><td>&lt; Section 4.3 &gt;</td><td><b>The method of selection:</b>
<b><u>Package – I</u></b>
Least Cost Selection (LCS)
<b><u>Package – II</u></b>
Quality and Cost Based Selection (QCBS) 70:30 method will be used to select the Bidder.
<b>Consortium or Subcontract is not allowed for participation in the tender.</b></td></tr>
<tr><td>&lt; Section 3.4.2 &gt;</td><td>RFP can be downloaded from http://www.ocac.in & http://www.odisha.gov.in. & www.enivida.odisha.gov.in The bidders are required to submit the bid processing fee of <b>Rs. 11,200 (Rupees Eleven Thousand Two Hundred Only)</b> in the form of a demand draft in favor of <b>“Odisha Computer Application Centre“</b> payable at <b>Bhubaneswar</b> from any of the Scheduled Bank along with the Proposal/bid.
Bidder has the option to submit the EMD through electronic mode to the mentioned Bank account and submit the proof of Bank Transfer screenshot in the PQ Bid Document
<table><tr><td>Bank A/c No.</td><td>149311100000195</td></tr><tr><td>Payee Name</td><td>Odisha Computer Application Center</td></tr><tr><td>Bank Name & Branch</td><td>Union Bank of Inidia, Acharya Vihar, Bhubaneswar</td></tr><tr><td>Account Type:</td><td>Savings</td></tr><tr><td>IFSC</td><td>UBIN0814938</td></tr></table></td></tr>
<tr><td>&lt; Section 3.4.3 &gt;</td><td><b><u>Package – I</u></b>
Earnest Money Deposit of amount <b>Rs. 2,00,000 (Rupees Two lakh Only)</b> through Demand Draft or Bank Guarantee in favor of “<b>Odisha Computer Application Centre</b>“ payable at <b>Bhubaneswar</b> from any of the Scheduled Bank.
<b><u>Package – II</u></b>
Earnest Money Deposit of amount <b>Rs. 15,00,000 (Rupees Fifteen lakhs Only)</b> through Demand Draft or Bank Guarantee in favor of “<b>Odisha Computer Application Centre</b>“ payable at <b>Bhubaneswar</b> from any of the Scheduled Bank.</td></tr>
</table>

<table>
<tr><th>Clause Reference</th><th>Topic</th></tr>
<tr><td></td><td>Bidder has the option to submit the EMD through electronic mode to the mentioned Bank account and submit the proof of Bank Transfer screenshot in the PQ Bid Document
<table>
<tr><td>Bank A/c No.</td><td>149311100000195</td></tr>
<tr><td>Payee Name</td><td>Odisha Computer Application Center</td></tr>
<tr><td>Bank Name & Branch</td><td>Union Bank of Inidia, Acharya Vihar, Bhubaneswar</td></tr>
<tr><td>Account Type:</td><td>Savings</td></tr>
<tr><td>IFSC</td><td>UBIN0814938</td></tr>
</table></td></tr>
<tr><td><b>< Section 3.5.2 ></b></td><td>The Proposal should be filled up by the Bidder in English language only.</td></tr>
<tr><td><b>< Section 4.3 ></b></td><td>Taxes: The bidder must quote price in Indian Rupees only. The bid price to be offered by the bidders must be inclusive of all taxes.</td></tr>
<tr><td><b>< Section 3.6.2 ></b></td><td>Proposals must remain valid till <b>180 days</b> after the last date of submission of the bids.</td></tr>
<tr><td><b>< Section 3.5.3 ></b></td><td>Proposals must be submitted not later than the following date and time: 30/03/2024 by 02:00 PM</td></tr>
</table>

2. Background Information

2.1. Basic Information

i. Odisha Computer Application Centre (OCAC) invites responses (“Tenders”) to this Request for Proposals (“RFP”) from (“Bidders”) who meet the minimum eligibility criteria as specified in this bidding document for “**Selection of Agency for Supply, Installation & Commissioning of Enterprise Security Solution for Cyber Security Operation Center (CSOC) Government of Odisha”.** OCAC is the Nodal Agency for this Government procurement.

ii. Proposals must be received not later than time, date and venue mentioned in the Fact Sheet. Proposals that are received after the date line WILL NOT be considered in this procurement process.

2.2. Project Background

To protect data, applications and ICT infrastructure of Odisha from security threats, Hon’ble Chief Minister, Sri Naveen Patnaik has inaugurated a state-of-the-art Next Generation Cyber Security Operation Centre (CSOC) at OCAC Tower in Bhubaneswar in the month of May 2022. CSOC has been set up by Electronics & Information Technology Department through Odisha Computer Application Centre, the Technical Directorate of E & IT Department.

The CSOC has been set up using the latest security technologies & tools. The system is fully automated and will secure government information and data from possible threats by hackers. State Data Centre (SDC), State Wide Area Network (SWAN) & Secretariat Network (SECLAN) have been integrated with CSOC.

3. Instructions to the Bidders

3.1. General

i. 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. Bidders and recipients of this RFP may wish to consult their own legal advisers in relation to this RFP.

ii. 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.

iii. 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.

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

3.2. Compliant Tenders / Completeness of Response

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

ii. 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.

3.3. Pre-Bid Meeting & Clarifications

3.3.1. Bidders Queries

i. OCAC shall hold a pre-bid meeting with the prospective bidders on **12/03/2024, 12:30** PM at through virtual mode only.

ii. The Bidders will have to ensure that their queries for Pre-Bid meeting should reach in e-mail id – : **gm_ocac@ocac.in** with a copy to **csoc@odisha.gov.in** only on or before **06/03/2024 by 05:00 PM**. Queries submitted after the scheduled date and time, shall not be accepted.

iii. Link will be provided to the interested bidders on request through email to gm_ocac@ocac.in (with a copy to csoc@odisha.gov.in and) by 12-March-2024, 11:00 AM.

iv. The representatives of Bidders (restricted to one person) may attend the Pre-bid meeting.

v. The queries should necessarily be submitted in the following format in excel file:

Sl. No.	RFP Document Reference(s) & Section	Page No.	Content of RFP requiring Clarification(s)	Points of Clarification
1.				
2.				

vi. OCAC shall not be responsible for ensuring that the bidder's queries have been received by them. Any requests for clarifications after the indicated date and time shall not be entertained by OCAC.

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

i. OCAC will endeavor to provide a timely response to all valid queries. However, OCAC makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does OCAC undertake to answer all the queries that have been posed by the bidders.

ii. At any time prior to the last date for receipt of bids, OCAC may, for any reason, modify the RFP Document by a corrigendum.

iii. The Corrigendum (if any) & clarifications to the queries from all bidders will be posted on the websites www.ocac.in, www.odisha.gov.in & https://enivida.odisha.gov.in /on **15/03/2024.**

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

v. In order to provide prospective Bidders reasonable time for taking the corrigendum into account, OCAC may, at its discretion, extend the last date for the receipt of Proposals.

3.4. Key Requirements of the Bid

3.4.1. Right to Terminate the Process

i. OCAC may terminate the RFP process at any time and without assigning any reason. OCAC makes no commitment, express or implied, that this process will result in a business transaction with anyone.

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

3.4.2. RFP Document Fees

i. RFP document can be downloaded from the website www.ocac.in & www.odisha.gov.in & www.enivida.odisha.gov.in The bidders are required to submit the Bid Processing Fee of Rs. 11,200/- (Rupees Eleven Thousand Two Hundred Only) inclusive of GST of 12% in shape of Demand Draft in favour of "Odisha Computer Application Centre" and payable at Bhubaneswar from any of the Scheduled Bank along with the Proposal. Proposals received without or with inadequate RFP Document fees shall be rejected.

ii. If a bidder participates in both Package – I & Package – II, then they need to submit Bid Processing Fee once and proof of fee submission should be submitted.

iii. The fee can also be paid through electronic mode to the following bank account.

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

3.4.3. Earnest Money Deposit (EMD)

i. Bidders shall submit, along with their Bids, EMD of **Rs. 2,00,000 (Rupees Two lakh only) for Package – I, Rs. 15,00,000 (Rupees Fifteen lakh only) for Package – II**, in form of a Demand Draft or Bank Guarantee (in the format specified **in Appendix I: Form 3)** issued by any Scheduled Bank in favour of "**Odisha Computer Application Centre**", payable at **Bhubaneswar**, and should be valid for **180 days** from the last date of submission of the RFP.

ii. Bidders, participated in each **Package** has to submit the respective EMD amount of that Package individually.

iii. EMD of all unsuccessful bidders would be refunded by OCAC within **90 days** of the bidder being notified as being unsuccessful. The EMD, for the amount mentioned above, of successful bidder would be returned upon submission of Performance Bank Guarantee as per the format provided in **Appendix III: Form 9.**

iv. The EMD amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.

v. The bid / proposal submitted without EMD, mentioned above, will be summarily rejected.

vi. The EMD may be forfeited:

- If a bidder withdraws its bid during the period of bid validity.
- In case of a successful bidder, if the bidder fails to sign the contract in accordance with this RFP.

vii. The fee can also be paid through electronic mode to the following bank account.

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

3.5. Submission of Proposal

3.5.1. Instruction to Bidders for Online Bid Submission

i. e-Nivida is a complete process of e-Tendering, from publishing tenders online, inviting online bids, evaluation and award of contract using the system. The instructions given below are meant to assist the bidders in registering on e-Nivida Portal and submitting their bid online on the portal.

ii. More information useful for submitting online bids on the e-Nivida Portal may be obtained at: https://enivida.odisha.gov.in

3.5.2. Guidelines for Registration

i. Bidders are required to enroll themselves on the eNivida Portal https://enivida.odisha.gov.in or click on the link "Bidder Enrolment" available on the home page by paying Registration Fees of Rs. 2500/- + Applicable GST.

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

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

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

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

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

vii. The scanned copies of all original documents should be uploaded in pdf format on e-tender portal.

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

3.5.3. Searching for Tender Documents

i. There are various search options built in the e-tender Portal, to facilitate bidders to search active tenders by several parameters.

ii. Once the bidders have selected the tenders they are interested in, then they can pay the Tender fee and processing fee (NON-REFUNDABLE) by net-banking / Debit / Credit card then you may download the required documents / tender schedules, Bid documents etc. Once you pay both fees, tenders will be moved to the respective 'requested' Tab. This would enable the e-Tender Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.

3.5.4. Preparation of Bids

i. Bidder should take into account any corrigendum published on the tender document before submitting their bids.

ii. Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.

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

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

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

3.5.5. Submission of Bids

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

ii. The bidder must digitally sign and upload the required bid documents one by one as indicated in the tender document as a token of acceptance of the terms and conditions laid down by the Department.

iii. The bidder must select the payment option as per the tender document to pay the Tender fee/ Tender Processing fee & EMD as applicable and enter details of the instrument.

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

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

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

vii. The uploaded bid documents become readable only after the tender opening by the authorized bid openers.

viii. Upon the successful and timely submission of bid click "Complete" (i.e. after clicking "Submit" in the portal), the portal will give a successful Tender submission acknowledgement & a bid summary will be displayed with the unique id and date & time of submission of the bid with all other relevant details.

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

3.5.6. Clarifications on using e-Nivida Portal

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

ii. Any queries relating to the process of online bid submission or queries relating to e-tender Portal in general may be directed to the Helpdesk Support.

iii. Please feel free to contact e-Nivida Helpdesk (as given below) for any query related to e-tendering.

Phone No.: 011-49606060

Email id: odishaenivida@gmail.com

3.6. General Instruction to Bidders

i. The bidders should submit their responses for each Package, as per the format given in this RFP.

ii. Bidders can participate in any Package as per their convenience.

iii. Please Note that Prices should not be indicated in the Pre-Qualification & Technical Proposal but should only be indicated in the Commercial Proposal.

iv. All the pages of the proposal must be sequentially numbered and must contain the list of contents with page numbers. Page references should be identified easily. If required, All the relevant parts should be highlighted in the bid documents. Any deficiency in the documentation may result in the rejection of the Bid.

v. All pages of the bid including, shall be digitally signed by the person or persons who is the signing authority of bid.

vi. A Proposal should be accompanied by a power-of-attorney / authorization in the name of the signatory of the Proposal.

vii. The Bidder(s) must submit the Form-4 (Compliance Sheet for Technical Proposal) in their official letterhead along with the Datasheet of the equipment quoted for Package – I

viii. The Bidder(s) must submit the Form-4 (Compliance Sheet for Technical Proposal) in their official letterhead along with the Datasheet of the equipment quoted along with other Technical Parameters for Technical Bid for Package – II

ix. Bidder has to submit Pre-Qualification -cum- Technical Proposal for Package-I. For Package-II bidder must submit Separate proposal for Pre-Qualification and Technical Proposal.

x. The Technical Proposal for Package – II should mandatorily have following information:

   a. Approach & Methodology
   b. Form 4: Compliance Sheet for Technical Proposal

3.7. Preparation and Submission of Proposal

3.7.1. Proposal Preparation Costs

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

3.7.2. Language

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

3.7.3. Deadline for Submission of proposals

Proposals, in its complete form in all respects as specified in the RFP, must be submitted to through www.enivida.odisha.gov.in by **30/03/2024 by 02:00 PM.**

3.7.4. Late Bids

i. Bids received after the due date and the specified time for any reason whatsoever, shall not be entertained and shall be returned unopened.

ii. The bids submitted by telex/telegram/ fax/e-mail etc. shall not be considered. No correspondence will be entertained on this matter.

iii. OCAC shall not be responsible for any postal delay or non-receipt/ non-delivery of the documents. No further correspondence on the subject will be entertained.

iv. OCAC reserves the right to modify and amend any of the above-stipulated condition/criterion depending upon project priorities and need.

3.8. Evaluation process

i. A Techno-Financial 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 of bid.

ii. The decision of the Procurement 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.

iii. The above-mentioned Committee may ask for meetings with the Bidders to seek clarifications on their proposals.

iv. The Procurement Committee reserves the right to reject any or all proposals on the basis of any deviations.

v. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.

3.8.1. Tender Opening

The Proposals submitted up to **30/03/2024, 02:00 PM** will be opened at **04:00 PM on 30/03/2024** before the Technical Committee.

3.8.2. Tender Validity

The offer submitted by the Bidders shall be valid for **180 days** from the last date of submission of Tender.

3.8.3. Tender Evaluation

i. Initial Bid scrutiny will be held and incomplete details as given below will be treated as non-responsive. If Proposals;

- Are not submitted in as specified in the RFP document
- Received without the Letter of Authorization/Power of Attorney
- Are found with suppression of details
- With incomplete information, subjective, conditional offers and partial offers submitted
- Submitted without the documents requested in the checklist
- Have non-compliance of any of the clauses stipulated in the RFP
- With lesser validity period

ii. All responsive Bids will be considered for further processing as below.

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

4. Criteria for Evaluation

4.1. Pre-Qualification (PQ) / Eligibility Criteria

All bids will primarily be evaluated on the basis of Prequalification Criteria. The Techno-Financial Committee will carry out a detailed evaluation of the Proposals. Only those bidders who qualify all Prequalification criteria are eligible for evaluation of technical bids. The bidder can bid for either one Package or both Packages as per their convenience.

Sl. No.	Basic Requirement	Specific Requirements	Documents Required
1.	Legal Entity	i. The bidder must be a company registered in India under Indian Companies Act 1956/2013 OR A Partnership firm registered under Indian Partnership Act, 1932.	– Valid copy of certificate of incorporation and registration certificates.

Sl. No.	Basic Requirement	Specific Requirements	Documents Required
		ii. The bidder office/s must have been in Odisha. iii. The bidder must be in operation in India since last 5 years as on 31st December 2023. The bidder must have GST registration & up-to-date Income Tax Return, Valid PAN Number as on 31st March 2023. **Note:** - In case of no Office in Odisha, self-certification stating that the awarded bidder shall have their office registered in Odisha within 30 days from the award of the contract.	– Copy of GST registration. – Copies of relevant Certificates of registration Income Tax / PAN – Any other necessary supporting documents
2.	Average Sales Turnover	Annual average Turnover during any three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows: a. **<u>Package – I</u> -** Minimum of **Rs. 10 Crores generated from IT Hardware supply and associated maintenance services.** b. **<u>Package – II</u> -** Minimum of **Rs. 30 Crores generated from Supply of Security Software Solution.**	Extracts from the audited Balance sheet and Profit & Loss; OR Certificate from the statutory auditor
3.	Net Worth	The net worth of the bidder in the last three financial years (showing for Average Annual Turnover) should be positive.	CA Certificate with CA's Registration Number / Seal indicating net worth of the firm
4.	OEM Experience	The OEM should have implemented at least 5 heterogeneous setups (means BFSI, Government /PSU/Autonomous body).	Customer PO copies, completion certificate and any feedback from the client.
5.	Technical Capability	The Bidder/OEM must have **successfully undertaken at least the following numbers of systems implementation engagement(s)** of value specified herein during the last three financial years i.e. 2020-21, 2021-22 & 2022-23:	Technical Capability: Work order/s along with Completion Certificates from the client

Sl. No.	Basic Requirement	Specific Requirements	Documents Required
		<u>Package – I</u> – One project of similar nature not less than the amount Rs. 1 crore; OR – Two projects of similar nature, each of which not less than the amount Rs. 60 Lakh. – Three projects of similar nature, each of which not less than the amount Rs. 40 Lakhs. – **<u>Package – II</u>** – One project of similar nature not less than the amount Rs. 3 crores; OR – Two projects of similar nature, each of which not less than the amount Rs. 2 Crores. – Three projects of similar nature, each of which not less than the amount Rs. 1.5 crore. – '**Similar Nature**' is defined as, **<u>Package – I</u>** "Similar Nature" is defined as: supply, installation & commissioning of Network and Security Components (Enterprise grade Firewall must be the major component within Security Components and should have functionalities asked in the RFP) Government/Semi Government/ PSU/ Scheduled Banks. **<u>Package – II</u>** "Similar Nature" is defined as: supply, installation & support of Enterprise Security Solution (Threat Intel Platform & Web Scanning Tool should be the major component and should be inclusive of all three solutions) Government/Semi Government/ PSU/ Scheduled Banks.	In case of ongoing project more than one year, Work order along with ongoing Certificates from the client.
	OEM Authorization	The bidder must attach Manufactures Authorization certificate specific to this tender & Back-to-back support letters from OEMs for providing Comprehensive support and services of the OEM's product covered under the RFP.	OEM MAF

Sl. No.	Basic Requirement	Specific Requirements	Documents Required
		MAF should contain the details of authorised signatory which includes Full name, designation, mobile no., email id) and should be digitally signed.	
6.	Quality Certifications	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022 Certifications.	Copy of valid certificate
7.	Undertaking on Authenticity of IT Hardware & peripherals and Enterprise Security Solutions	The bidder should submit an undertaking on Authenticity of IT Hardware & peripherals and Enterprise Security Solutions, on Rs. 100/- Non-judicial stamp paper.	As per Form - 6
8.	Local Office	The bidder should have presence in Odisha with support Centers.	– A Self Certified letter by an authorized signatory; OR – Undertaking for setting up Local office with in 30 days of issuance of LOI/ PO / Work Order from OCAC.
9.	Blacklisting	The bidder must not have been blacklisted by any Department of Government of Odisha or Government of India. The bidder must also disclose full details of any blacklisting by Central or State PSUs/Undertakings/Autonomous Organizations or under a declaration of ineligibility for corrupt or fraudulent practices in last two years 'as on' **31/01/2024'**.	A Self Certified letter by an authorized signatory.
10.	Performance	The Bidder/OEM must not have any record of poor performance, abandoned work, having inordinately delayed completion and having faced Commercial failures etc. for any State Government or Government of India Organization /	A Self Certified letter

Sl. No.	Basic Requirement	Specific Requirements	Documents Required
		Department during last 5 years as on '**31/01/2024**'.	
11.	Fees	i. The Bidder must have submitted **Rs.11,200/- (Rupees Eleven Thousand Two Hundred only)** towards the cost of the Bid Processing Fee. ii. The Bidder must have furnished the EMD of **Rs. 2,00,000/- (Rupees Two lakh only)** for **Package – I,** EMD of **Rs. 15,00,000/- (Rupees Fifteen lakh only)** for **Package – II** and; iii.EMD of **Rs. 17,00,000/- (Rupees Seventeen lakh only)** for **Both Packages.**	i. Demand Draft ii. Demand Draft / Bank Guarantee (As per **Form – 3**) iii. Electronic Fund Transfer Copy

4.2. Technical Qualification Criteria

Bidders who meet the pre-qualifications/ eligibility requirements would be considered as qualified to move to the next stage of evaluation, i.e. Technical evaluation. Financial evaluation of those bidders will be made who qualify in the Technical evaluation. The Product offered should meet all the technical and functional specifications given in the **"Form 4: Compliance Sheet for Technical Proposal".** Non-compliance to any of the technical and functional specification will attract rejection of the proposal.

Response except Yes(Y) or No(N) is not acceptable. If any bidder provides response other than Y or N, the same will be treated as Not Available (NA). Bidders, whose bids are responsive to all the items in the Compliance Sheet of Technical Proposal and meet all the technical and functional specifications, would be considered as technically qualified.

If any non-compliance is found during technical evaluation in respect of any or more items in both Package, OCAC reserves the right to place work order excluding those items.

Note: - *Technical Evaluation will be done, individual Package wise*

4.2.1. Technical Evaluation Criteria for Package – I

i. Bidder must quote all the products/equipment mentioned in the Bill of Materials. Otherwise, the bid will not be considered.

ii. Form-4 (Compliance Sheet for Technical Proposal) in OEM official letterhead along with the Datasheet of the equipment quoted.

iii. Bidder must furnish tender-specific Manufacture Authorization Form against the entire item mentioned in the Bill of Material.

4.2.2. Technical Evaluation Criteria for Package – II

i. Bidder must quote all the products/equipment mentioned in the Bill of Materials. Otherwise, the bid will not be considered.

ii. Form-4 (Compliance Sheet for Technical Proposal) in OEM official letterhead along with the Datasheet of the equipment quoted.

iii. Bidder must furnish tender-specific Manufacture Authorization Form against the entire item mentioned in the Bill of Material.

iv. The Bidder/OEM must have experience with the Proposed requirements and should be implemented and running in Public/Government entity in India. (The bidder may submit Copy of original PO, Contract Completion Certificate or Installation Report or Credential letter from client working specifying project completion).

v. The bidder should furnish documentation in technical bid and make demonstration/presentation on the proposed solution as per following parameters before bid evaluation committee. Based on the documentation and presentation/demonstration mark shall be awarded.

vi. All the bidders who secure a Technical Score of 70 or more will be declared as technically qualified. The commercial bids of only the technically qualified bidders will be opened for further processing.

vii. The bidder with the highest Technical bid Score (H1

viii.) will be awarded 100 score.

ix. Technical Score of a Bidder (Tn) = {(Technical Bid Score of the Bidder / Technical Bid Score of H1) X 100} (Adjusted up to two decimal places)

x. Technical Evaluation Scoring Matrix as follows:

Sl	Evaluation Criterion	Maximum Marks	Supporting Document
1	Bidder/OEM should have experience in Threat Intel Solution for SOC environment as per functionalities of Threat Intel Platform Mentioned in RFP - Section 21.5.2.1	20 Each Project – 10 Marks	Work Order
2	Bidder/OEM should have experience in Threat Integration Platform for SOC environment as per functionalities of Threat Integration Platform Mentioned in RFP - Section 21.5.2.2	20 Each Project – 10 Marks	Work Order
2	Bidder/OEM should have experience in Supply, Installation and Support of Web Scanning Tool for Data Centre- Section 21.5.2.3	20 Each Project – 10 Marks	Work Order

Sl	Evaluation Criterion	Maximum Marks	Supporting Document
3	Presentation- Understanding of the project, technical design, approach methodology, solution specifications, Training Plan	40	Technical Document: 1. Design Architecture of Proposed Solution 2. Resilience of proposed architecture, approach and methodology 3. Future scalability Presentation: 1. Bidder's understanding on project scope. 2. Bidder's knowledge and experience to deliver vis-à-vis scope of the assignment. 3. Project timeline, implementation framework on the proposed solution 4. Bidder's ability to provide crisp and clear answers with strong content Submission of Presentation Copy to OCAC after Technical Presentation

4.3. Commercial Bid Evaluation

i. The Financial Bids of technically qualified bidders in respective Package will be opened on the prescribed date.

4.3.1. Commercial Bid Evaluation for Package - I

i. The Bidder who submits the lowest Commercial bid, shall be selected as the L1 bidder (for respective Package and shall be called for further process leading to the award of the assignment.

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

iii. Prices quoted in the bid must be firm and final and shall not be subject to any modifications, on any account whatsoever.

iv. All the required items must be listed and priced separately in the financial bid. If a financial bid shows items listed but not priced, their prices shall be assumed to be included in the prices of other items.

v. Evaluation will be made on the basis of Total bid price inclusive of all taxes. The bidder has to quote Tax(s) as applicable in the Tax Columns of Financial Bid Format. Evaluation will be done on the basis of Grand Total cost of respective Package (inclusive of all Taxes) [Total cost = (Unit cost + Taxes as applicable)].

vi. In case of a Tie of the bid price for L1, both the bidders shall be called for further negotiation, then whose ever price becomes L1 will be awarded the contract.

vii. Any conditional commercial bid would be rejected.

viii. Errors & Rectification: Arithmetical errors will be rectified on the following basis: “If there is a discrepancy between the unit price and the total price of any item that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected accordingly. In case of multiple items, grand total price shall be corrected adding the sub-total costs of each item. If there is a discrepancy between words and figures in respect of unit price, the amount in words will prevail”.

4.3.2. Commercial Bid Evaluation for Package - II

i. Bidders will be selected through QCBS - Quality & Cost Based Selection with Technical and Financial ratio of 70:30.

ii. The Financial Bids of the technically qualified bidders (who score more than 70 marks in Technical Evaluation) will be opened on the prescribed date in the presence of bidders’ representatives.

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

iv. The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately.

v. Any conditional bid would be rejected.

vi. Errors & Rectification: Arithmetical errors will be rectified on the following basis: “If there is a discrepancy between the unit price and total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail. If the bidder does not accept the correction of error, its bid will be rejected”.

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

viii. The bidder with lowest qualifying financial bid (L1) will be awarded 100 score. Financial score for other bidders will be evaluated using the following formula;

ix. Financial Score of a Bidder (Fn)={(Financial Bid of L1/ Financial Bid of the Bidder) X 100} (Adjusted up to two decimal Places)

4.3.3. Final Bid Evaluation for Package - II

i. The technical and financial evaluation scores secured by each bidder will be added using weightages of 70% and 30% respectively to compute composite score.

ii. The formula for the calculation of the Composite score

Bn = 0.70 * Tn + 0.30* Fn
Where:
Bn = overall score of bidder
Tn = Technical score of the bidder (out of maximum of 100 marks)
Fn = Normalized financial score of the bidder

iii. The Bidder securing the Highest Composite Bid Score will be adjudicated with the Best Value Bidder for award of the project.

5. Appointment of Enterprise Security Solution Provider

5.1. Award Criteria

OCAC will award the Contract to the successful bidder **(H1)** whose proposal is determined to be substantially responsive in the respective Package and has been determined as the most responsive bid as per the process outlined above.

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

OCAC reserves the right to accept or reject any proposal, and to annul the tendering process / Public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for OCAC action.

5.3. Notification of Award

Prior to the expiration of the validity period, OCAC will notify the successful bidder, in individual Package, in writing or by fax or email, that its proposal has been accepted. In case the tendering process / public procurement process has not been completed within the stipulated period, OCAC may like to request the bidders to extend the validity period of the bid.

The notification of award will constitute the formation of the contract. Upon the successful bidder furnishing Performance Bank Guarantee, OCAC will notify each unsuccessful bidder and return their EMD.

5.4. Performance Bank Guarantee (PBG)

i. The selected bidder will submit a Performance Bank Guarantee (PBG), within **15 days** from the Notification of award, for a value equivalent to 10**%** of the total order value.

ii. The Performance Bank Guarantee needs to be furnished on a yearly basis and to be valid up to 15 months in the first year and needs to be renewed accordingly on yearly basis before the expiry period of 15 months. Total validity period of the PBG shall be 63 months from the date of submission of PBG. The selected bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the project and Warranty period.

iii. In case the selected bidder fails to submit performance Bank guarantee within the time stipulated, OCAC at its discretion may cancel the order placed on the selected bidder without giving any notice and forfeit the EMD.

iv. In that event, OCAC, at its discretion, may award the Contract to the next best value bidder with the discovered H2 Price, in case the bidder is agreed and whose offer is valid.

v. OCAC shall invoke the performance Bank Guarantee in case the selected Vendor fails to discharge their contractual obligations during the project period or OCAC incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.

vi. Performance Bank Guarantee shall be returned after 3 months of warranty period completion.

vii. No interest will be paid by OCAC on the amount of performance Bank Guarantee

5.5. Signing of Contract

Post submission of Performance Bank Guarantee by the successful bidder, OCAC shall enter into a contract, incorporating all clauses, pre-bid clarifications and the proposal of the bidder between OCAC and the successful bidder.

5.6. Monitoring of Contract

i. OCAC will monitor the progress of the contract during its delivery period.

ii. During the delivery period OCAC shall keep a watch on the progress of the contract and shall ensure that the quantity of goods and service delivery is in proportion to the total delivery period given in the Work order.

iii. If a delay in delivery of goods and service is observed, a performance notice would be given to the selected bidder(s) to speed up the delivery and LD will be charged accordingly.

iv. The selected bidder shall not assign or sub-let his contract or any substantial part thereof to any other agency without the permission of OCAC.

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

Failure of the successful bidder to agree with the Draft Legal Agreement and Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event OCAC may award the contract to the next best value bidder or call for new proposals from the interested bidders. In such a case, OCAC shall invoke the PBG of the bidder.

6. Fraudulent and Corrupt Practices

i. The Bidders and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the Selection Process. Notwithstanding anything to the contrary contained in this RFP, OCAC shall reject a Proposal without being liable in any manner whatsoever to the Bidder, if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice (collectively the “Prohibited Practices”) in the Selection Process. In such an event, OCAC shall, without prejudice to its any other rights or remedies, forfeit and appropriate the Bid Security or Performance Security, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to the Authority for, inter alia, time, cost and effort of the Authority, in regard to the RFP, including consideration and evaluation of such Bidder’s Proposal.

ii. Without prejudice to the rights of OCAC under Clause above and the rights and remedies which OCAC may have under the LOI or the Agreement, if a Bidder is found by OCAC to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the Work Order or the execution of the Agreement, such Bidder shall not be eligible to participate in any tender or RFP issued by OCAC/ Any Department of State Govt. during a period of 2 (two) years from the date of such Bid.

iii. For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them:

a. “corrupt practice” means (i) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the Selection Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of OCAC who is or has been associated in any manner, directly or indirectly with the Selection Process.

b. “fraudulent practice” means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process;

c. “coercive practice” means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person s participation or action in the Selection Process;

d. “undesirable practice” means (i) establishing contact with any person connected with or employed or engaged by OCAC with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest; and

e. “Restrictive Practice” means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.

7. Conflict of Interest

The Vendor shall disclose to OCAC in writing, all actual and potential conflicts of interest that exist, arise or may arise in the course of performing the Service(s) as soon as practical after it becomes aware of that conflict.

i. OCAC considers a conflict of interest to be a situation in which a party has interests that could improperly influence that party's performance of official duties or responsibilities, contractual obligations, or compliance with applicable laws and regulations. In pursuance of OCAC's Procurement Ethics requirement that bidders, suppliers, and contractors under contracts, observe the highest standard of ethics, OCAC will take appropriate actions against the bidder(s), if it determines that a conflict of interest has flawed the integrity of any procurement process. Consequently, all bidders found to have a conflict of interest shall be disqualified.

ii. A bidder may be considered to be in a conflict of interest if the bidder or any of its affiliates participated as a consultant in the preparation of the solicitation documents/RFP for the procurement of the goods and services that are the subject matter of the bid.

iii. It may be considered to be in a conflict of interest with one or more parties in the bidding process if

a. they have controlling shareholders in common; or

b. it receives or have received any direct or indirect subsidy from any of them; or

c. they have the same legal representative for purposes of the Bid; or

d. they have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about or influence on the Bid of another Bidder or influence the decisions of the tendering authority regarding this bidding process.

8. Terms and Conditions: Applicable Post Award of Contract

8.1. Termination Clause

8.1.1. Right to Terminate the Process

OCAC reserves the right to cancel the contract placed on the selected bidder and recover expenditure incurred by OCAC under the following circumstances: -

i. The selected bidder commits a breach of any of the terms and conditions of the bid.

ii. The bidder goes into liquidation, voluntarily or otherwise.

iii. If the selected bidder fails to complete the assignment as per the timelines prescribed in the RFP and the extension if any allowed, it will be a breach of contract. OCAC reserves its right to cancel the order in the event of delay and forfeit the bid security as liquidated damages for the delay.

iv. In case the selected bidder fails to deliver the quantity as stipulated in the delivery schedule, OCAC reserves the right to procure the same or similar product from alternate sources at the risk, cost and responsibility of the selected bidder, after 2 weeks of cure period.

v. OCAC reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking the bank guarantee under this contract.

8.1.2. Consequences of Termination

i. In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], OCAC shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the Vendor shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution/continued execution of the scope of the Contract.

ii. Nothing herein shall restrict the right of OCAC to invoke Performance Bank Guarantee and other guarantees, securities furnished, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available to OCAC under law or otherwise.

iii. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

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

i. Except as provided under clause "Force Majeure", if the selected bidder fails to deliver any or all of the Goods or perform the Related Services within the period specified in the Contract, OCAC may without prejudice to all its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to the percentage specified in sub clause (iv) below for each week or part thereof of delay until actual delivery or performance, up to a maximum deduction of the percentage specified in sub clause (iv). Once the maximum timeline is reached, the Purchaser may terminate the Contract pursuant to clause "Termination".

ii. The time specified for delivery in the tender form shall be deemed to be the essence of the contract and the selected bidder shall arrange goods supply and related services within the specified period.

iii. The delivery and completion period may be extended with or without liquidated damages if the delay in the supply of goods or service is on account of hindrances beyond the control of the selected bidder to be determined by OCAC.

   a. The supplier/ selected bidder(s) shall request in writing to OCAC giving reasons for extending the delivery period of service, if he finds himself unable to complete the supply of goods or service within the stipulated delivery period or is unable to maintain prorate progress in the supply of goods or service delivery. This request shall be submitted as soon as a hindrance in delivery of goods and service occurs or within **15 days** from such occurrence but before expiry of stipulated period of completion of delivery of goods and service after which such request shall not be entertained.

b. OCAC shall examine the justification of causes of hindrance in the delivery of goods and service and the period of delay occurred due to that and recommend the competent authority on the period of extension which should be granted with or without liquidated damages.

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

d. It shall be at the discretion of the competent authority to accept or not to accept the supply of goods and/ or services rendered by the contractor after the expiry of the stipulated delivery period, if no formal extension in delivery period has been applied and granted. The competent authority shall have right to cancel the contract with respect to undelivered goods and/ or service.

iv. In case of extension in the delivery and/ or completion period is granted with full liquidated damages, the recovery shall be made on the basis of following percentages of value of goods which the selected bidder has failed to supply or complete : -

No.	Condition
1	For delay in delivery of materials beyond the delivery schedule mentioned in the work order**, LD @ 0.5%** per week or part thereof for the pending materials order value up to maximum **5%** will be deducted.

a. The maximum amount of liquidated damages shall be 5% of the total order value.

b. OCAC reserves its right to recover these amounts by any mode such as adjusting from any payments to be made by OCAC to the bidder.

8.3. Service Level Agreement and Penalties

8.3.1. SLA for Package - I

i. SLA defines the terms of the successful bidder’s responsibility in ensuring the performance of the hardware, software & all other accessories supplied as per the **Scope of Work** as specified in the RFP document based on the agreed Performance Indicators as detailed in the Agreement.

ii. The Bidder shall provide comprehensive, end-to-end service including supply, warranty and replacement of the defective IT Hardware & peripherals in case of physical damage until delivered at OCAC. No reason shall be entertained (unless those mentioned in Force Majeure) in case of un-availability of any service given in the **Scope of Work** in this RFP and the appropriate **penalty** shall be levied.

iii. The selected bidder and OCAC shall regularly review the performance of the services being provided by the selected bidder and the effectiveness of this SLA.

iv. The following measurements and targets shall be used to track and report performance on a regular basis. The targets shown in the following tables are applicable for the entire duration of the Contract /Project, failing which the selected bidder(s) is liable to be penalized:

Sl. No.	**Type of Incident**	**Target Resolution Time**	**Penalty**
1.	**Any defect in IT Hardware & peripherals or any of its part**	<=T+7 days	No penalty
		> T+ 7 days	0.5% of cost of the IT Hardware & peripherals will be deducted per week upto maximum 5% of faulty IT Hardware/Peripheral cost.
		> T + 60 Days	If the selected bidder fails to rectify a defect within 90 days, OCAC may proceed to take such remedial action as may be necessary (including Invocation of PBG), in addition to other recourses available in terms and conditions of the contract and bidding document

Note: -

1. ***The upper limit of the penalties due to default in SLA Warranty is 5% of the entire PO value.***
2. ***T is the time when user reports the defect with the IT Hardware and peripherals by complain log in through web/ help desk. The bidder shall generate a Ticket on receipt of complaint and has to keep proper record of 'Complaint Date' & 'Issue Resolution Date.***

8.3.2. SLA for Package - II

Sl	**Definition**	**Measurement Level**	**Target**	**Penalty**
1	Application / Software availability	Monthly	>=99.99%	No Penalty

Sl	Definition	Measurement Level	Target	Penalty
2	Application / Software availability	Monthly	< 99.99%	0.5 % Cost of Tool Value deducted from O&M Cost
3	Dashboards availability	Monthly	Shall be available with >=99.99 % functionalities.	No Penalty
4	Dashboards availability	Monthly	< 99.99%	0.5 % Cost of Tool Value deducted from O&M Cost
5	Version Upgrade Major/ Minor for all Software / Middleware	The Operations Team have to have version upgrades of all underlying software / Middleware as per respective OEM recommendations & Publish the Quarterly version upgrade calendar for the same. Failure to comply with Version upgrade calendar will attract penalties.	Breaches of Version upgrade	Penalty of Rs.1000 per day for delay in version upgrade of (OS, Server, Solution, protocol etc.) per day. deducted from O&M Cost
6	OEM Health Check	Yearly	Health check, if not conducted by the OEM representative once in a year	Penalty of Rs. 2,000 will be charged for each such solution for each defaulted month will be imposed. deducted from O&M Cost

Sl	Definition	Measurement Level	Target	Penalty
7	Brand Monitoring.	Alert notification should be within 30 minutes of detection. For routine observations, a consolidated mail on a daily basis to be sent		For any miss in the monthly average 30 minutes from detect to notify, 0.125% of O&M Cost
8	Dark web Monitoring	Alert notification should be within 30 minutes of detection. For routine observations, a consolidated mail on a daily basis to be sent.		For any miss in the monthly average 30 minutes from detect to notify, 0.125% of O&M Cost
9	Takedown of Phishing sites/ Fake Mobile Applications etc.	Takedown from the time of go ahead for takedown from OCAC: a) After 3 weekdays and less than or equal to 5 weekdays b) Beyond 5 weekdays Note: Weekdays would mean Mon-Fri.		a) 1.5 times the unit price of every such take down service. b) 0.5 times the unit price of every such take down service

8.4. Dispute Resolution Mechanism

The Bidder and OCAC shall endeavor their best to amicably settle all disputes arising out of or in connection with the Contract in the following manner:

i. The Party raising a dispute shall address to the other Party a notice requesting an amicable settlement of the dispute within **seven (7) days** of receipt of the notice.

ii. The matter will be referred for negotiation between OCAC and the Authorized Official of the Bidder. The matter shall then be resolved between them and the agreed course of action documented within a further period of **15 days.**

iii. In case, it is not resolved between OCAC and the bidder, it will be referred to Principal Secretary to Govt., E&IT Department., Govt. of Odisha for negotiation and his decision would be final and binding for both the parties.

iv. In case any dispute between the Parties, does not settle by negotiation in the manner as mentioned above, the same may be resolved exclusively by arbitration and such dispute may be submitted by either party for arbitration within **20 days** of the failure of negotiations. Arbitration shall be held in **Bhubaneswar** and conducted in accordance with the provisions of the Arbitration and Conciliation Act, 1996 or any statutory modification or re-enactment thereof. Each Party to the dispute shall appoint one arbitrator each and the two arbitrators shall jointly appoint the third or the presiding arbitrator.

v. The "Arbitration Notice" should accurately set out the disputes between the parties, the intention of the aggrieved party to refer such disputes to arbitration as provided herein, the name of the person it seeks to appoint as an arbitrator with a request to the other party to appoint its arbitrator within **45 days** from receipt of the notice. All notices by one party to the other in connection with the arbitration shall be in writing and be made as provided in this tender document.

vi. Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the Parties unless the award otherwise provides. The Bidder shall not be entitled to suspend the Service/s or the completion of the job, pending resolution of any dispute between the Parties and shall continue to render the Service/s in accordance with the provisions of the Contract/Agreement notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings.

8.5. Notices

Notice or other communications given or required to be given under the contract shall be in writing and shall be faxed/e-mailed/hand-delivery with acknowledgement thereof, or transmitted by pre-paid registered post or courier.

8.6. Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the selected bidder 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:

i. Natural phenomenon, including but not limited to floods, droughts, earthquakes and epidemics.

ii. Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos.

iii. Terrorist attack, public unrest in work area provided either party shall within 10 days from occurrence of such a cause, notifies the other in writing of such causes. The bidder or OCAC shall not be liable for delay in performing his/her obligations resulting from any force majeure cause as referred to and/or defined above. Any delay beyond 30 days shall lead to termination of contract by parties and all obligations expressed quantitatively shall be calculated as on date of termination. Notwithstanding this, provisions relating to indemnity, confidentiality survive termination of the contract.

8.7. Failure to agree with Terms and Conditions of the RFP

Failure of the successful bidder to agree with the Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event OCAC shall invoke the EMD/PBG of the selected bidder and may award the contract to the next best value bidder or call for new proposals from the interested bidders.

9. Details on Scope of Work for Package - I

9.1. Scope of Work

i. Supply, install and commission of Enterprise Security Solution for CSOC as per Bill of Quantity mentioned, complying with the technical specification given, along with software licenses, accessories and necessary documents/manuals will be delivered at OCAC.

ii. The Bidder shall ensure the safe delivery of the equipment up to the designated place of installation. Any transit insurance, labor, road permits etc., if required for the same, shall be arranged by the Bidder at no extra cost to OCAC.

iii. The implementation of this project is extremely critical for CSOC wherein the entire demographics of the Network/server infrastructure setup are going to be realigned. Hence the bidder is expected to use the services of OEM nominated professional services who will be present and be involved in the critical tasks from day 1(One). The OEM professional services are supposed to impart the following services but not limited to the same.

iv. The bidder(s) shall not quote and supply any hardware/ software that is likely to be declared as End of Service/ Support for Thirty-Six months from the date of bid submission. If any of the hardware/ software is found to be declared as End of Service/ Support in the period mentioned above, then the bidder shall replace within 7 days, all such hardware/ software with the latest ones having equivalent or higher specifications without any financial obligation to OCAC.

v. The OEM shall ensure the seamless installation and integration of the offered solution without disturbing the on-going working of the existing equipment and applications.

vi. The installation & commissioning shall include all components and sub-components like cables (such as fiber, ethernet etc.), connectors, tools, transceiver, H/w & S/w licenses, accessories and other components (required for commissioning of the solution as a part of the RFP requirement) should be supplied by the bidder.

vii. The solution should be deployed in high availability with active-active mode. Further the offered solution should be Robust, Secure and Scalable.

viii. Testing of the equipment's commissioning and ensuring proper functioning at all levels.

ix. The proposed solution should have the latest technological features and standards.

x. The solution is compatible with all standard SIEM solutions. The central management can send/exchange log to the SIEM solution for correlation.

xi. The license should be in the name of Odisha Computer Application Centre (OCAC).

9.1.1. Warranty & Support

i. The Bidder should have a Back-to-Back support agreement with OEM, till the completion of the warranty period of the entire equipment to ensure the smooth functioning and to achieve the highest uptime on the offered solution.

ii. Advanced replacement of hardware.

iii. Software updates and upgrades at no extra cost to OCAC.

iv. On-site support from the Bidder.

9.1.2. Training and Handholding

i. The Selected Bidder shall impart necessary handholding for effective usages of the equipment if any when required by OCAC.

ii. The successful bidder will be required to hold administration training for at least 4 Officials / Management team of OCAC by the OEM, covering basic concept, configuring as per the different specs, report generations in different customized formats like time wise, severity wise, protocol wise, source/destination etc., log analysis, definition &software version update/upgrade. The training will be provided on premises at CSOC and OEM has to provide all licenses for the same.

9.1.3. Project Deliverables, Milestones & Time Schedule

i. The time specified for delivery and other activities as mentioned in the table below shall be deemed to be the essence of the contract and the successful bidder shall arrange supplies and provide the required services within the specified period.

ii. It should be noted that any delay in the project timelines shall cause Liquidated Damages to the Agency.

Sl. No.	Activity / Mile stone	Delivery Schedule
1	Delivery of Equipment	**4 Weeks** from date of issue of Purchase Order to the Bidder
2	Installation, Configuration & Integration	**6 Weeks** from date of issue of Purchase Order to the Bidder
3	UAT, Sign-off	**8 Weeks** from date of issue of Purchase Order to the Bidder
4	Training (Knowledge Transfer)	**Within 10 Weeks** from date of issue of Purchase Order to the Bidder

Note: -Total time for completion (Supply, installation and commissioning) of the contract / project is 12 weeks. In case the project is not completed in time, a penalty of 0.5% per week (pro-rata basis considering one week is 7 days) maximum up to 8 weeks will be applicable. After that Odisha Computer Application Centre (OCAC) will be free to cancel the contract. Once the contract is cancelled the PBG amount will be forfeited by OCAC.

9.2. Indicative Bill of Quantity (BOQ)

Sl. No.	Item Details	Qty	UoM
1	Firewall (FW) in High Availability (HA)	02 (Fully Populated)	Nos
2	24 Port L2 Network Switch	01 (Fully Populated)	Nos
3	Optical Patch Cable, OM4 multi-mode Duplex LC-LC, 10 meters	20	Nos.
4	Optical Patch Cable, OM4 Single-mode Duplex SC-LC, 10 meters	20	Nos.
5	CAT6 UTP Patch Cord – Factory Crimped, 3 meters	20	Nos.
6	CAT6 UTP Patch Cord – Factory Crimped, 10 meters	10	Nos.

10. Details on Scope of Work for Package - II

i) The Bidder must be compliant with "Technical evaluation criteria" and be able to propose and implement the project as per the requirements specified in this document

ii) Supply of the proposed tool licenses as mentioned in the RFP.

iii) Support the departments in the deployment, integration, configuration of the proposed tool licenses with their respective applications.

iv) Solution should be easily integrated with existing SIEM solution of CSOC.

v) Solution should have capabilities to integrate with leading SIEM solutions.

vi) Perform configuration / customization / modifications or adding new dashboards / alerts for getting more clarity into the issues.

vii) Provide updates and upgrades of the product during the entire contract period, at no additional cost.

viii) Both bidder and OEM will be responsible for the maintenance, configuration and fault free operations of supplied infrastructure i.e. hardware, software and its maintenance during the warranty and post warranty.

ix) Any technical glitch/ issue in installed infrastructure of the solution (i.e. hardware and software, OS/DB etc.) should be attended on priority and should be covered under warranty/AMC.

x) The license should be in the name of Odisha Computer Application Centre (OCAC).

10.1. Training and Handholding

i. The Selected Bidder shall impart necessary handholding for effective usages of the equipment if any as and when required by OCAC.

ii. The successful bidder will be required to hold administration training for at least 4 Officials / Management team of OCAC by the OEM, covering basic concept, configuring as per the different specs, report generations in different customized formats like time wise, severity wise, protocol wise, source/destination etc., log analysis, definition &software version update/upgrade. The training will be provided on premises at CSOC and OEM has to provide all licenses for the same.

iii. OEM training should be initiated at the time of installation and configuration and afterwards it should be Conducted twice in Each Year for entire duration of Contract period. There should be a gap of six months between subsequent training sessions. Also, in case any critical functionality updates of the product should be carried out during the contract period.

10.2. Project Deliverables, Milestones & Time Schedule

i. The time specified for delivery and other activities as mentioned in the table below shall be deemed to be the essence of the contract and the successful bidder shall arrange supplies and provide the required services within the specified period.

ii. It should be noted that any delay in the project timelines shall cause Liquidated Damages to the Agency.

Sl. No.	Activity / Mile stone	Delivery Schedule
1	Delivery of Tools	**4 Weeks** from date of issue of Purchase Order to the Bidder
2	Installation, Configuration & Integration	**8 Weeks** from date of issue of Purchase Order to the Bidder
3	Training (Knowledge Transfer)	**Within 10 Weeks** from date of Purchase Order to the Bidder
4	Operation & Maintenance (O&M)	O&M period will start after successful completion of Installation, Configuration & Integration

10.3. Indicative Bill of Quantity (BOQ)

Sl. No.	Item Details	Qty	UoM
1	Threat Intel Solution	01	Solution
2	Threat Integration Platform	01	Solution
3	Web Application Scanning Tool (cost should include the cost for Enterprise Licenses, integration with end user departments, updates, upgrades, dashboard configuration and support etc.)	01	Unit

i. Web Application Vulnerability Scanning tool should be On – Premises Deployment. For Same necessary Hardware and Peripheral installation components need to be provided by bidder and bidder should include the Hardware and installation cost in Tool Price as UoM mentioned as Unit

ii. OCAC will facilitate Only Space, Power and Cooling.

11. Right to alter Quantities

OCAC reserves the right to give repeat order to the **L1/H1 bidder in Respective Package** for maximum upto **20% of ordered quantity**, if required, within the tender validity period of **180 days** from the last date of submission of bid under same terms and conditions with same Specifications and Rate. Any decision of OCAC in this regard shall be final, conclusive and binding on the bidder. If OCAC does not purchase any of the tendered articles or purchases less than the quantity indicated in the bidding document, the bidder(s) shall not be entitled to claim any compensation.

12. Confidential Information

OCAC and Selected bidder shall keep confidential and not, 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 Contract, whether such information has been furnished prior to, during or following completion or termination of the Contract.

13. Specifications and Standards

i. All articles to be supplied shall strictly conform to the specifications, trademark laid down in the tender form and wherever articles have been required according to ISI/ ISO/ other applicable specifications/ certifications/ standards, those articles should conform strictly to those specifications/ certifications/ standards. The supply shall be of best quality and description. The decision of the competent authority/ purchase committee whether the articles supplied conform to the specifications shall be final and binding on the selected bidder.

ii. Technical Specifications:

a. The Selected bidder shall ensure that the goods and related services comply with the technical specifications and other provisions laid down in the RFP & the work order.

b. The Selected bidder shall be entitled to disclaim responsibility for any design, data, drawing, specification or other document, or any modification thereof provided or designed by or on behalf of the Purchaser, by giving a notice of such disclaimer to the Purchaser.

c. The goods and related services supplied under this Contract shall conform to the standards mentioned in bidding document and, when no applicable standard mentioned, the standard shall be equivalent or superior to the official standards whose application is appropriate to the country of origin of the Goods.

14. Packing and Documents

i. The Selected bidder shall provide such packing of the Goods as is required to prevent their damage or deterioration during transit to their final destination. During transit, the packing shall be sufficient to withstand, without limitation, rough handling and exposure to extreme temperatures, salt and precipitation, and open storage. Packing case size and weights shall take into consideration, where appropriate, the remoteness of the final destination of the Goods and the absence of heavy handling facilities at all points in transit.

ii. The Bidder shall be responsible for any defect in packing and any material found damaged / defective at the delivery points and those are to be replaced by the selected bidder within 2 weeks without any financial obligations to OCAC.

15. Transit Insurance

The IT Hardware and peripherals to be supplied under the Contract shall be fully insured against any loss during transit from OEM site to OCAC. The insurance charges will be borne by the supplier and OCAC will not pay such charges.

16. Authenticity of Equipment(s)

i. The selected bidder shall certify (as per Form 6) that the supplied goods are brand new, genuine / authentic, not refurbished, confirm to the description and quality as specified in this bidding document and are free from defects in material, workmanship and service.

ii. If during the contract period, the said goods be discovered counterfeit/ unauthentic or not to confirm to the description and quality aforesaid or have determined (and the decision of OCAC in that behalf will be final and conclusive), notwithstanding the fact that the purchaser may have inspected and/ or approved the said goods, the purchaser will be entitled to reject the said goods or such portion thereof as may be discovered not to confirm to the said description and quality, on such rejection the goods will be at the selected bidder's risk and all the provisions relating to rejection of goods etc., shall apply.

iii. Goods accepted by the purchaser in terms of the contract shall in no way dilute purchaser's right to reject the same later, if found deficient in terms of the this clause of the contract.

17. Limitation of Liability

Except in cases of gross negligence or willful misconduct: -

a. neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier/ selected bidder to pay liquidated damages to the Purchaser; and

b. the aggregate liability of the selected bidder to the Purchaser, whether under the Contract, in tort, or otherwise, shall not exceed the amount specified in the Contract, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the supplier/ selected bidder(s) to indemnify the Purchaser with respect to patent infringement.

18. Change in Laws & Regulations

i. Unless otherwise specified in the Contract, if after the date of the Invitation for Bids, any law, regulation, ordinance, order or bylaw having the force of law is enacted, promulgated, abrogated, or changed in Odisha/ India, where the Site is located (which shall be deemed to include any change in interpretation or application by the competent authorities) that subsequently affects the Delivery Date and/ or the Contract Price, then such Delivery Date and/or Contract Price shall be correspondingly increased or decreased, to the extent that the Supplier has thereby been affected in the performance of any of its obligations under the Contract.

ii. Notwithstanding the foregoing, such additional or reduced cost shall not be separately paid or credited, if the same has already been accounted for in the price adjustment provisions where applicable.

19. Change Orders and Contract Amendments

i. OCAC may at any time order the selected bidder through Notice in accordance with clause "Notices" above, to make changes within the general scope of the Contract in any one or more of the following: -

   a. drawings, designs, or specifications, where Goods to be furnished under the Contract are to be specifically manufactured for the Purchaser;
   b. the place of delivery; and
   c. the related services to be provided by the selected bidder.

ii. If any such change causes an increase or decrease in the cost of, or the time required for, the selected bidder's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or in the Delivery and Completion Schedule, or both, and the Contract shall accordingly be amended. Any claims by the selected bidder for adjustment under this clause must be asserted within thirty (30) days from the date of the selected bidder's receipt of the Purchaser's change order.

iii. Prices to be charged by the selected bidder for any related services that might be needed but which were not included in the Contract shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the selected bidder for similar services.

20. Payment Terms and Procedure

20.1. Paying Authority

i. The payments as per the Payment Schedule covered herein above shall be paid by OCAC. However, Payment of the Bills would be payable, on receipt of advice/confirmation for satisfactory delivery/installation/re-installation, and inspection/service report from the authorized official of Odisha Computer Application Centre (OCAC)

ii. The selected bidder's request for payment shall be made to OCAC in writing, accompanied by invoices describing, as appropriate, the goods delivered and related services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfillment of all the obligations stipulated in the Contract.

iii. Due Payments shall be made promptly by OCAC, generally within **Forty Five (45) days** after submission of an invoice and other supporting documents in order.

iv. The currency or currencies in which payments shall be made to the supplier/ selected bidder(s) under this Contract shall be Indian Rupees (INR) only.

v. All remittance charges will be borne by the selected bidder.

vi. In case of disputed items, disputed amount shall be withheld and will be paid only after settlement of the dispute.

vii. Advance Payments will not be made.

viii. Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this bidding document, will be deducted from the payments for the respective milestones.

ix. Taxes, as applicable, will be deducted at source, from due payments, as per the prevalent rules and regulations

20.2. Payment Schedules for Package - I

Sl.	Project Milestone	Payment (%)	Documents Required
1	Delivery of Equipment & Verification	60% of the contract value	1. Original Delivery Challan 2. Original Invoice (In triplicate)
2	Installation, Configuration, Integration	30% of the contract value	1.Installation Certificate duly certified by Nodal officer nominated by OCAC
3	Training (Knowledge Transfer) & UAT	10% of the contract value	1. Training (Knowledge Transfer) 2. Warranty Certificate for 5 years from UAT 3. Back-to-back support document from OEM

20.3. Payment Schedules for Package - II

Sl.	Project Milestone	Payment (%)	Documents Required
1	Delivery of Solution	60% of the contract value	1.Original Delivery Challan 2. Required License in the Name of OCAC
2	Installation, Configuration, Integration & UAT	20% of the contract value	1.Installation Certificate duly certified by Nodal officer nominated by OCAC 2. Successful UAT certified by Nodal officer nominated by OCAC
3	Training (Knowledge Transfer)	10% of the contract value	To be released in 5 installments after successful completion of Training by OEM for each tool each year for the period of 5 Years

Sl.	Project Milestone	Payment (%)	Documents Required
			Bidder should organize the training from OEM after Installation, Configuration, Integration & UAT
4	Operation and Maintenance Support	100% of O&M Cost	To be released in 10 installments after completion of each 6 months for a period of 5 Years The O&M date will start after the successful completion of Installation, Configuration, Integration completion & UAT Submission of Successful O&M completion document certified by Nodal officer nominated OCAC

21. Appendix I: Pre-Qualification –cum – Technical Bid Templates

21.1. General

The bidders are expected to respond to the RFP using the forms given in this section and all documents supporting Pre-Qualification–cum-Technical Evaluation Criteria. Pre-Qualification Bid – cum – Technical Proposal shall comprise of following forms:

Forms to be used in Pre-Qualification Proposal

Form 1: Compliance Sheet for Pre-qualification Proposal

Form 2: Particulars of the Bidders

Form 3: Bank Guarantee for Earnest Money Deposit (EMD)

Forms to be used in Technical Proposal

Form 4: Compliance Sheet for Technical Proposal

Form 5: Letter of Proposal

Form 6: Undertaking on Authenticity of IT Hardware and peripherals

21.2. Form 1: Compliance Sheet

21.2.1. Package - I

For Package – I, the Form -1 will be considered as Pre-Qualification – cum – Technical proposal.

Sl. No.	Basic Requirement	Documents Required	Complied (Yes /No)	Reference & Page Number
1.	Document Fee	Demand Draft		
2.	Earnest Money Deposit	Demand Draft / Electronic Transfer to Bank account copy / Bank Guarantee **(Form 3)**		
3.	Power of Attorney/ Authorization	Copy of Power of Attorney/ Authorization in the name of the Authorized signatory		
4.	Particulars of the Bidders	As per **Form 2**		
5.	Average Sales Turnover in IT Hardware supply and associated maintenance services in three financial years	Extracts from the audited Balance sheet and Profit & Loss; OR Certificate from the statutory auditor		
6.	The net worth of the bidder in the last three financial years	CA Certificate with CA's Registration Number/ Seal indicating net worth of the firm		
7.	Technical Capability	Work Order + Completion Certificates from the client;		
8.	Quality Certifications	ISO 9001:2015		

Sl. No.	Basic Requirement	Documents Required	Complied (Yes /No)	Reference & Page Number
		ISO 27001:2013 / ISO 27001:2022		
9.	Legal Entity	Copy of Certificate of Incorporation, GST registration, PAN, IT return		
10.	Blacklisting & Performance	A self-certified letter		
11.	Undertaking on Authenticity of IT Hardware & peripherals (To be filled by the bidder (On Rs. 100/- Non-judicial stamp paper))	As per **Form - 6**		

21.2.2. Package - II

For Package – II, the Form -1 will be considered as Pre-Qualification proposal. All the requirements of Pre-Qualification should be submitted along with Form-1 for Pre-Qualification proposal.

Sl. No.	**Basic Requirement**	**Documents Required**	**Complied (Yes /No)**	**Reference & Page Number**
1.	Document Fee	Demand Draft		
2.	Earnest Money Deposit	Demand Draft / Electronic Transfer to Bank account copy / Bank Guarantee **(Form 3)**		
3.	Power of Attorney/ Authorization	Copy of Power of Attorney/ Authorization in the name of the Authorized signatory		
4.	Particulars of the Bidders	As per **Form 2**		
5.	Average Sales Turnover in IT Hardware supply and associated maintenance services in three financial years	Extracts from the audited Balance sheet and Profit & Loss; OR Certificate from the statutory auditor		
6.	The net worth of the bidder in the last three financial years	CA Certificate with CA's Registration Number/ Seal indicating net worth of the firm		
7.	Quality Certifications	ISO 9001:2015, ISO 20000:2018 ISO 27001:2013 / ISO 27001:2022		
8.	Legal Entity	Copy of Certificate of Incorporation, GST registration, PAN, IT return		
9.	Blacklisting & Performance	A self-certified letter		
10.	Undertaking on Authenticity of IT Hardware & peripherals (To be filled by the bidder (On Rs. 100/- Non-judicial stamp paper))	As per **Form - 6**		

21.3. Form 2: Particulars of the Bidders

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

21.4. Form 3: Bank Guarantee for Earnest Money Deposit (EMD)

< Location, Date >

To,

The General Manager (Admn)
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
P.O.- RRL, Bhubaneswar - 751013
EPBX: 0674-2567280/2567064/2567295
Fax: +91-0674-2567842

Whereas << name of the bidder >> (hereinafter called the Bidder) has submitted the bid for Submission of RFP # << RFP Number >> dated << insert date >> for << name of the assignment >>(hereinafter called "the Bid") to Odisha Computer Application Centre

Know all Men by these presents that we <<>> having our office at << Address >> (hereinafter called "the Bank") are bound unto the << Nodal Agency >> (hereinafter called "the Purchaser") in the sum of Rs. << Amount in figures >> (Rupees << Amount in words >> only) for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this << insert date >>

The conditions of this obligation are:

1. If the Bidder having its bid withdrawn during the period of bid validity specified by the Bidder on the Bid Form; or
2. If the Bidder, having been notified of the acceptance of its bid by the Purchaser during the period of validity of bid

a. Withdraws his participation from the bid during the period of validity of bid document; or
b. Fails or refuses to participate for failure to respond in the subsequent Tender process after having been short listed;

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

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

NOTHWITHSTANDING ANYTHING CONTAINED HEREIN:

I. Our liability under this Bank Guarantee shall not exceed Rs. << Amount in figures >> (Rupees << Amount in words >> only)

II. This Bank Guarantee shall be valid upto << *insert date* >>)

III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before << *insert date* >>) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

Seal:

Date:

21.5. Form 4: Compliance Sheet for Technical Proposal

(Note: All the specifications below are minimum specifications and higher specifications shall be used wherever necessary/ required. Deviation on higher side shall only be considered and no extra weightage shall be awarded for such deviations.)

21.5.1. PACKAGE-I

21.5.1.1. Specification for Firewall

Minimum 50% and 20% Local Content required for qualifying as Class 1 and Class 2 Local Supplier respectively)			
S.No.	**Technical Specification**	**Compliance (Yes/No)**	**Offered Parameter**
	Make :- **Model :-**		
1	**Hardware Specification**		
1.1	Device Should be 1RU; 19 Inch Rack mountable		
1.2	The appliance should have multicore processor based architecture.		
1.3	The appliance should have minimum 8 x 10/100/1000 Base T Ethernet Port		
1.4	The appliance should have minimum 8 Ports of 1Gbps SFP		
1.5	The appliance should have minimum 4 Ports of 10Gbps SFP+		
1.6	The appliance should have minimum 1 x Expandable Slots support with optional 8 x SFP/Copper or 4 x SFP+ Port for future requirement		
1.7	The appliance should have minimum 1 x Management port		
1.8	The appliance should have minimum internal storage of 1TB SSD for Logs & Reports or better.		
1.9	The appliance Should have Minimum 16GB DDR4 Memory or better		
1.10	The appliance should have Dual Redundant internal Power Supply from Day1		
1.11	The appliance should have Hot Swappable Power Supply		
1.12	Proposed solution should have bandwidth quota and time quota for manageability of users		
1.13	The Firewall should be Network DLP compliant for future upgradation		
2	**License Deliverable /Description**		
2.1	Need 5 Years / 60 Month H/W Warranty with stateful inspection and firewall policies to control access of ports and hosts or network.		
2.2	The firewall should have provision for future upgradation of Next generation firewall license		

	which include Next Generation Intrusion Prevention System (IPS), Zero Day Protection / Advance Malware protection, Web Security Essentials / URL Filtering ; Antivirus, URL Filter, Application Filtering, Anti-Spam, user identity, and Basic 24x7 Support		
3	**Performance Capacity –Minimum**		
3.1	The appliance should have minimum Firewall Throughput of 70 Gbps or better		
3.2	The appliance should be able to handle minimum 500K new session per second or better		
3.3	The appliance should be able to handle minimum 10 Gbps NGFW Throughput or better		
3.4	The appliance should have minimum Antivirus Throughput of 12 Gbps or better		
3.5	The appliance should have minimum IPS Throughput of 12 Gbps or better		
3.6	The appliance should have minimum Firewall IMIX Throughput of 28 Gbps or better		
3.7	The appliance should have minimum VPN Throughput of 13 Gbps or better		
3.8	The appliance should have minimum 40000 Number of IPSec VPN Peers supported (Site to Site)		
3.9	The appliance should have minimum 40000 Number of IPSec VPN Peers supported (Client to Site)		
3.10	The appliance should have minimum 10000 Number of SSL VPN Peers supported (Client to Site)		
3.11	The appliance should have minimum 20M Concurrent Session/Concurrent Connection		
3.12	The appliance Should support 85+ Web categories for future upgradation of URL filter license		
3.13	The appliance Should support 5000+ application Signature for future upgradation of APP filter license		
3.14	The appliance Should support 25000+ IPS Signature for future upgradation of Next generation IPS license		
3.15	The proposed system should have the future option to integrate with cloud-based management system to manage Firewall. Both solutions should be from the same OEM.		
3.16	The Proposed solution should have a future flexibility / option to provide complete policy enforcement and visibility of roaming users and should restrict the remote user from disabling it.		
3.17	The Proposed solution should have a future flexibility to apply organization policy framework to the remote users and ideally, it should control the Web and Application filter of the remote user		
Other Terms & Conditions			

1	Supply, Installation, Integration, testing commissioning and training as per site requirements shall be done by the bidder.		
2	The proposed appliance should come from firewall appliance family which has more than 5 years of ICSA labs certification/NSS/NDP/ Indian Standard, IC3S/Common Criteria		
3	OEM should be ISO 9001-2015 & ISO 27001:2013 Certified.		
4	The Firewall appliance should have certifications like NDPP / ICSA / EAL4 or more		
5	The proposed OEM should Comply with Make in India as per Public Procurement Act (Preference to Make in India)		
6	The product shall comply minimum 60% and Above Local content or higher.		
7	The product shall have Indian Standard, IC3S/Common Criteria (provided by STQC in India common-criteria- certification-0) or Alternatively from International equivalents, NDPP or NSS or ICSALabs, at least one of them should be provided while bidding.		
8	Certificate of authorization (MAF) for this bid must be submit with bid. Bidders need to submit MAF from respective OEM is mandatory, otherwise authority should have right to cancel the Bidder.		
9	The bidder should be ISO certified organization.		
10	The bidder should have their own certified technical engineer of quoted product from the respective OEM for installation & warranty support station in Eastern India. The details of the engineer must be furnished with the bid.		
11	The bidder should have their registered office in eastern India to ensure immediate support during downtime.		
12	During Technical evaluations or Prior to Price bid open, Bidder need to do 7-15 Days POC if asked; POC will be at our premises and during POC if found product is not complying with mentioned requirement than authorities has the right to reject the bid during technical evaluations.		

21.5.1.2. Specification for 24 Port Layer-2 Managed Switch

S.No.	Technical Specification	Compliance (Yes/No)	Offered Parameter
	Make:- **Model:-**		
1	Switch architecture should be Fixed Form factor/ stackable based		
2	Switch should have wire-speed, non-blocking and distributed forwarding on all the ports.		
3	Switch should have minimum of 12 x 10/100/1000 Mbps RJ45, 6x1G SFP(MM), 6x10G SFP+(SM) plus 4 x1/10G SFP+ (MM)uplink ports. Trans receiver module from day one. (All QSFP/SFP+/SFP Transceiver modules should be from same Switch OEM)		
4	Switch should support min 16K MAC addresses and min 1000 active VLANs. Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs.		
5	Switch should have full Layer 2 features and support spanning tree protocols standards like STP (IEEE 802.1d), MSTP(IEEE 802.1s) RSTP (IEEE 802.1w) etc. LACP/IEEE802.3ad, ACL, QoS and IGMPv1/v2/v3 from day one.		
6	Switch should have Static Routing for IPv4 & IPv6 from day1.Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128 on hardware for all ports.		
7	Should support 1K IGMP Groups.		
8	Should support 8 queues per port and security protocols like RADIUS, TACACS/TACACS+, AAA & SSH. Always-on POE to that supplies POE power even during schedule reboot.		
9	The OEM must feature in the Leaders segment of the Gartner Magic Quadrant for Data Center Enterprise Networking published for last 3 consecutive years		
10	Switch should be quoted with 5 years direct OEM TAC support and Next Business Day hardware shipment.		
11	Equipment should be minimum TEC certified or IPV6 Ready Logo Certified. IPV6 Routing & Management features should be active from Day-1.		
12	Comprehensive Onsite OEM Warranty for 5 Years		
13	All the required licenses for making the Switches fully functional should be bundled		

21.5.1.3. Project Citation Format

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

NB:-

Please attach supporting documents like Workorder , Completion Certificate Etc.
This should be part of Pre Qualification – Cum – Technical Bid for Package - I

21.5.2. PACKAGE-II

21.5.2.1. Specification for Threat Intel Solution

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
1	Platform	Vendor must have Minimum 10 years expertise in anti–malware research/Threat Research		
		Role Based Access Control		
		Platform should provide the UI in multiple languages(Eg.(i) Arabic (ii) Chinese (both simplified and traditional script) (iv) Farsi (Persian) (v) French (vi) German (vii) Japanese (viii) Russian (ix) Spanish (x) English) & support Summarization & translation of the information		
		The OEM solution must comply to the following certifications: A. ISO/IEC 27701:2019 for Privacy Information Management System B. ISO 9001 Compliant		
		Multitenancy		
		Solution should provide AI summary of ecosystem to help in risk remediation & better decision making		
		Should provide negligible noise & false positives Signal to Noise Ratio (SNR) > 90%		
		The Vendor must have a local representative or distributor in the country who is operating locally for at least 5 years.		
		AI Summary should be provided on executive dashboard help decision making & remediation steps		
		Single dashboard should provide visibility of all the required use cases		
		Platform should use AI algorithm to provide summary of any post, chatter or article on Darkweb & Surface web posted in any language & also assign a risk score on top of that		
		Vendors' staff assigned to the project must hold professional certifications related to cybersecurity such as: GNFA, GCIH, CISM, CISA, CISSP.(Preferred)		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		Display the searched data in various types of views such as list view, timeline based view , MAP based view and Source based View		
2	Threat Intelligence Feed Requirement	Threat intelligence feed should identify new global threats feeds from it's own Global Sensors and Honeypots network as well along with premium threat intel sources, including but not limited to Malicious IP Addresses, Domain, URL, Filename, File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like Lat long, AS Number, ISP, Country, etc.		
		Platform should provide an IOC Lookup feature, where customer will get IOC Risk Score, Confidence Score, Source details, TA profile & IOA		
		The solution shall provide information in following categories (if possible): • Brief description of the revealed vulnerabilities, threats, traces of compromise, as well as current cybercriminal and cyberespionage activity against the Customer's assets. • Network Reconnaissance and Vulnerability Analysis • Malware and Cyber–Attack Tracking Analysis • Staff, Data Leakage Analysis • Underground Activities Analysis • WHOIS Analysis • MX Records Analysis • Subdomains Analysis Email addresses Analysis • Social Network Analysis Additional information on detailed technical analysis results.		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		The solution should allow to search URL's / Domains and provide the following general information: • Status – Shows whether the requested URL can be classified as malicious, good, or not categorized. • IPv4 count – Number of known IP addresses related to the requested URL. • Files count – Number of known malicious / all files. • Created – URL creation date. • Expires – URL expiration date. • Domain – Name of the upper–level domain. • Registration organization – Name of the registration organization. • Registrar name – Name of the domain name registrar. • Owner name – Domain owner name. • Category – Category of the requested URL.		
		The solution should allow to search IP addresses and provide the following general information: • Status – Shows whether the requested IP address generates malicious activity. • Hits – Hit number (popularity) of the requested IP address. • First seen – Date and time when the requested IP address appeared in expert systems statistics for the first time • Threat scope – Probability that the requested IP address will appear dangerous (0 to 100). • Owner name – Name of the requested IP address owner. • Owner ID – ID of the requested IP address owner. • Created – Date when the requested IP address was registered. • Updated – Date when information about the requested IP address was last updated. • Category – Category of the requested IP address		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		A) In-house Premium Threat Advisories that cover Ransomware Campaigns and TTPs, Threat Actors and their TTPs, APT Groups, Data Breaches, Vulnerability analysis, Malware campaigns B) Solution should provide near real time alerts on Breaches for various Industries & geographies in the form of NewsFlashes on Dashboard		
		Threat identified with the solution should have (but not limited) the following attributes: • Date of identification • Risk score • Category • Object associated with threat • Threat name (if known) • Threat description Recommendation (if applicable)		
		Platform should provide the visibility on the Hacktivists and other state sponsored campaigns		
		Platform should provide OT/ICS Threat Intel feeds with interactive dashboard.		
		Platform should have a Threat Library section, providing detailed intel on global Advanced Persistent Threat Groups, Ransomware groups,Threat Actors, Tools they use, their Aliases, IOCs, Country of Origin, Target Industry & Target Geography for effective monitoring and tracking.		
		The solution must be able to look for if an Exploit or Code is publicly available or underground discussions, alleged selling, or alleged privately held code observed.		
		Feeds from the platform should be integrated with client solutions like: SIEM, SOAR, TIP, EDR in STIX TAXII format or via Web API		
		The Threat feeds must be auto updated at least once every 1 hour for IP addresses, once every 2 hours for domains and URLs , once every day for hashes and once every week for CVEs		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		The Threat feeds must be collected from multiple third party sources both OSINT and paid, deduplicated and then offered to OCAC via API based. integration.		
		Feeds from the platform should be integrated with client solution's like: SIEM , SOAR, TIP, EDR in STIX TAXII format or via Web API"		
		The feeds should not be limited to open-source information but should extend to closed (non-public) information		
		The feeds should not only provide a series of individual data points but also correlate and analyze disparate data points and draw informed conclusions		
3	Cyber-threat monitoring of surface and dark web	Detect if any data is leaked using OCAC's public assets such as Intellectual Properties, Domains, Subdomains, mail-id and OCAC defined keywords. The solution should have the capability to analyze data from multiple languages as mentioned in technical specification		
		Crawl through dark web forums to identify if there is any data leak from OCAC or if someone is asking information pertaining to OCAC or OCAC assets.		
		Identify if any of OCAC employee's and assets credentials are leaked or sold online. The system must update the list as and when any new breaches occur and report at the earliest. Moreover, the proposed solution should support customized and automated alerts and reports with information such as IP address, Machine Name, Threat Vector used etc		
		Monitor the email IDs of OCAC's top executive for any potential credential leaks		
		Monitor open security forums, like pastebin, GitHub, Open Bug Bounty etc., ingesting data from multiple code sharing and open security forums and report any such code leaks having mention of OCAC or its public assets such as Intellectual Property, Domains, Subdomains, etc		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		Perform basic level of vulnerability scanning – like open ports, misconfigured SSLs, leaking object storages in public cloud, XSS vulnerabilities and report the same on a daily basis. Scan all Internet-facing infrastructure and identify/ report on critical security issues. Any misconfigured subdomains and IP address must be monitored closely for possible data leakage		
		Maintain a comprehensive inventory and fingerprint of all OCAC Internet- facing digital assets such as domains, related subdomains, respective IP addresses, logo, associated web and mobile applications. OCAC shall be able to add to the assets, if so required		
		Platform should provide the feasibility to customize the severity logic for alerts & events based on the Threat lanscape of customer		
		Apart from Portal & emails, event notification should be available on all of the below channels at a desired frequency on Whatsapp/SMS/Mobile app		
		Monitor data sharing sites like Pastebin, Scribd etc and report any sensitive data associated with the client		
4	Darkweb & Deepweb Monitoring	Bidder should provide an early intelligence on the Compromised endpoints, Cookies & Session keys of customer internal application available for sale in Darkweb Marketplaces		
		Vendor should also provide clear distinction between internal assets or internal employees & the other stakeholders like customers & partners in the case of exposed credentials		
		Intelligence provided must have reference to the source of information including Dark web and Deep web and Paste bin sites, either through a direct link to the source or a cached copy without Customer actually going onto Dark web to look for evidence.		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		The Platform must be able to create, monitor, automate alert and report for threat on Dark Web but is not limited to, the following: -Employee compromised credentials -Sensitive information Leakage such as Username Password Secret token access keys -Compromised PII such as Email ID, Phone number and Address. -information about the compromised system such as device ID, host name, IP address etc to help in forensic investigation -Malware and Malicious Infrastructure related to Customer domain -Private / Sensitive Documents relating to the business. -Hacking documents/tools specifically targeting client; -Leaked Source Code. -Intellectual property exposed or leaked -Copyright / Trademark infringement. -Technical Information / Data that could be used to compromise corporate systems. - Mentions of IP Addresses and Infrastructure -Use of BIN and other PII serial numbers to identify client-related accounts and credentials. -Stolen / Compromised Login Credentials and Customer Account Information. - Exposure in 3rd Party Breaches		
		The platform should incorporate a range of multi- layered monitoring services and analysis techniques and correlates data across a range of resources including: - .onion sites, I2P sites and alternative networks; - Dark Net blogs, forums, chat rooms; - Infostealer Marketplaces, Logs and Cookies - IRC conversations; - Black market and criminal auction sites - Ransomware forums - Telegram		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		- Discord - Paste sites		
		Monitor the global list of websites and mobile applications. Monitor domains like .com/ .org/ .co.in/ .in & other domains and alert the moment any website tries to purpurate the OCAC website		
		Hacktivist tracking and intelligence correlation - understand the Hacktivist world and alert OCAC of any news that has an impact on OCAC		
		Monitor to identify fraudulent techniques, scams, data trade and vulnerabilities targeting OCAC systems		
		The provider should be able to provide the facility to analysis the historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity)		
		The solution must display images in the search results from sources such as Twitter, LIVEUAMAP, Ransomware extortion sites such as ALPHV, Arvin Club etc and link it to the current context. For image results there should be an option to disable viewing/blurring of images or reporting it.		
		Platform should provide intelligence from Internet traffic analysis to look for possible exfiltration or C2 extraction from OCAC PUBLIC IP range.		
		The solution must provide information on IOC with reliability score, detection quality or risk score. Scores must be justified with rational behind the given scores. Scores must be dynamic to represent the automated real-time risk of the said IOC for confident decision making and response.		
		The solution must be able to look for Exploit Proof of Concepts on selective technologies & sources like Dark Web and Underground forums and help to prevent Zero day exploits.		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
5	Brand Intelligence	Social Media Monitoring: The platform should monitor all the major social media platform, including, but not limited to; Twitter, Facebook, YouTube, Instagram, LinkedIn, Tiktok,Vimeo, RSS All data sources should be collectively analyzed for the use of Customer's brand. These should be reviewed by bidder's / OEM's Security Analysts, manually verified, and evaluated to determine the extent of any abuse or fraud. If abuse is suspected, Customer should be immediately notified to take the site down or seek to have the post removed via the normal Incident Response channel.		
		Fake Customer Service Contact details - Fake Social Media profiles - Fake Domains/URLs and Web pages - Fake recruitment drives & Hiring Scams - Fake Videos or Images using client Logos		
		Platform should provide : Website Watermarking Website Defacement monitoring		
		The Bidder/OEM should be member of International Anti-Phishing Working Group (APWG). Solution should provide the visibility of DNS records, Whois records, MX records, screenshot tagged to a typoquatted domain Solution should provide Domain Watclisting feature, to get instant alert whenever there's a change in the status of domain Platform should be capable of doing Image/Logo monitoring to identify profile impersonation Finding domains and emails mentions on Code Repository websites like Github etc CXOs fake social media profiles, posts, pages and groups, takedown is also expected here.		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
6	Take Down Service	Platform should monitor & do a Takedown of the following cases (including but not limited to): - Phishing sites & Campaigns - Fake Mobile Apps on Appstore, Playstore & other 3rd party Application stores - Fake Customer Service Contact details - Fake Social Media profiles - Fake Domains/URLs and Web pages - Fake recruitment drives - Fake Videos or Images using client Logos		
		The Bidder/OEM should provide take down support for minimum 500 take downs for the duration of the contract.		
		Takedown service should be worldwide.		
		OEM Should have their own in-house takedown mechanism and not rely on 3rd-party services.		
7	Attack Surface management	Platform should discover & then monitor the complete Tech Inventory of customer, including but not limited to: — Cloud Buckets — Domains — IPs — IP Ranges — Subdomains — DNS Records (A, AAAA, CNAME, SOA, MX, NS, TXT etc.) — Digital Certificates — Trackers — Keywords — Technologies — Emails — Executives (Cxx / VPs)		
		Vendor should provide Vulnerability Intelligence which will include: a) Vulnerability source information, extensive references, links to Proof of Concept code and solutions b) Vulnerability Intel on 3rd party software products c) Vulnerability Prioritization		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		The Platform must monitor all of Customer's Public Infrastructure continuously and provide report on • Exploitable Vulnerabilities from known & Unknown assets • CVE/ SSL Expiry • Shadow IT • Sensitive Open Port • Certificate Issues • Misconfigured Devices • The platform must scan the internet for finding RDP, VNC, xserver		
		Platform should also monitor cloud infrastructure of the customer & provide the visibility of the issues & vulnerabilities. Tool should maintain the dynamic cloud inventory		
		The Platform must monitor misconfigured cloud repositories, public folders and peer-to-peer networks for data that could represent leaked confidential or sensitive information.		
		Platform should monitor exposed sensitive codes on all of the platforms listed below:(Not Limited to) Github BitBucket Postman Docker Hub		
		Bidder should have it's own Internet Scanner & data pipeline to monitor the Attack Surface exposure of the customer, it should not be dependent on any 3rd party to provide this service		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		Bidder should Provide Public Assets information's like(Not Limited to) *Screenshot *Web Applications details *WAF and CDN Information *Favicon Detect -Vulnerabilities and Critical Open -Virtual Host (Shadow IT Asset) - Local file inclusion -Path Traversal - Default Logins - Web App Misconfigurations - Insecure Design - Broken Authentication		
		The solution should show information about spam attacks in which the requested object is attached to email messages.		
		Platform should support application security scanning of web applications (OWASP Top 10 vulnerabilities) & should provide visibility into Botnet Detection		
8	Intelligence on CVEs and Vulnerabilities	The solution should be able to create watch list of software tech stack of OCAC and alert for vulnerabilities on the following type of threats a)New critical vulnerability announcement and real-world risk of the vulnerability at Pre-NVD level. b)Trending Vulnerabilities in specific Industries c)Vulnerabilities exploited in the wild by Malwares d)CVEs with low, medium or high potential for exploitation. e)Exploitation has been reported or confirmed to widely occur.		
		The vulnerability threat intelligence should be bundled with tools to import vulnerability scan results in CSV format.		
		The vulnerability solution must have a dashboard view that identifies all types of vulnerabilities with a risk and exploit rating.		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
9	Intelligence on Leaked Credentials	The solution must provide the following details in respect of a leaked credentials for a given authorized organizational domain for the following: a) Leaked Username or Leaked Email Address b)Full unsalted hashes in encrypted format (eg SHA1, MD5, SHA256, NTLM) c)Clear text password hint (first 2 characters) or full cleartext password to enable credential owner to identify and remediate their use of the exposed password as part of point a) d)Details on applications URL for which the credential works		
		The solution should provide information about the breach events such as first and last downloaded date , compromise date linked to these dumps (zero or more.)		
		The solution must offer details around the compromised host such as computer name, OS username, IP Address, File Path of Malware, AV and Host Firewall details, Malware name etc if available with the credential		
		The solution must provide relevant dashboards to highlight exposure timelines and exposure details like top domains, technologies, dominant malware etc		
		The solution must have option to restrict view of cleartext password for limited admin users only		
10	Threat Analysis	Detailed execution map with highlighted MITRE ATT&CK techniques		
		Clicking links in documents for Microsoft Office (Word, Excel, PowerPoint, Publisher, Outlook) and Adobe Reader		
		Possibility to export the analysis details in STIX, JSON, CSV formats		
		Network activities (SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, SOCKS sessions; HTTP(s), requests and responses		
		Detailed threat intelligence with actionable context for every revealed indicator of compromise (IOC)		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		The analysis platform should calculate the reputation score of the sample and reveal its genetics and code attribution. This provides insights into the origin of the sample and can enable its attribution to possible authors.		
11	Browser Extension Requirements	The solution should be offered with a web browser extension for Chrome, Mozilla Firefox and Chromium-based Microsoft Edge that should scan any webpage in real time, identify relevant entities, and presents a list of entities detected along with their risk scores.		
		The browser extension must highlight the total number of IOCs(IOCs like IP, URL, hash, domain and CVE) are identified on the page with their associated risk scores. IOCs should be highlighted on the page itself using different color codes for critical, medium and low severity.		
		Browser extension must ensure that the information is organized in order by risk score Risk score, Triggered risk rules and evidences that assist in prioritization of IOCs being shown on the page for reducing triage time for analyst.		
		The browser extension must have capability to block potentially malicious links on the webpage being reviewed by the analyst		
		The browser extension must have the option to enable or disable automatic detection of IOCs like IP, Domain, URL, hash and vulnerability (CVE)		
		The browser extension must work with the following solutions Anomaly ThreatStream, ArcSight ESM, ELK (Dashboard only), MISP, Qualys, The Hive Project, VirusTotal etc		
		The browser extension must have the capability to export the IOC such as IP, Domains, URLs, Hash files and vulnerabilities into separate CSV files directly from the browser plugin.		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		The browser extension must have the capability to upload suspicious file URLs for detonation and analysis to OEM offered sandbox solution.		
12	Sandbox	Dynamic Malware Sandboxing should be available: The service should support malware sandboxing by allowing users to a. Upload suspicious files to the platform and download a detailed file behavior analysis report and network analysis report for each uploaded file b. The analysis report should contain risk score of the file, relevant indicators of compromise such as IP addresses, domains or C2 URLs, suspicious network connections, usage of potentially malicious API and files downloaded or dropped on the disk upon successful execution c. The sandbox should protect organizational privacy by not uploading the file to any publicly accessible repository or third party B. The sandboxing should support operating systems such as Windows, Linux, Mac IoS & Android at a minimum. C. The service should support automated analysis of at-least 50 samples per day D. The service provider should provide analyst support for report interpretation and explanation as and when required.		
13	Reports	All TTPs described in the reports should be mapped to MITRE ATT&CK, enabling proved detection and response through developing and prioritizing the corresponding security monitoring use cases, performing gap analyses and testing current defenses against relevant TTPs		
		Intel on threat actor profiles Including suspected country of origin and main activity, malware families used, industries and geographies targeted, and descriptions of all TTPs used, with mapping to MITRE ATT&CK		

Signature & Seal of the Bidder

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		Should provide technical descriptions about the latest threats during ongoing investigations, before release to the general public		
		Detailed descriptions of threats targeting financial infrastructures and the corresponding attack tools being developed or sold by cybercriminals on the Dark Web in various geographies		
		Should provide C Level executive Summary which includes in geography, Data exfiltration analysis and victim analysis		
		The report should include conclusions and recommendations too.		
14	Training	The OEM of the solution must provide access to unlimited online training to the offered solution including YARA rules.		
		The course should teach how to write effective Yara rules, how to test them and improve them to the point where they find threats .		
15	Support	The solution must be provided with 24/7 access to the support team via web, email and phone		
		The solution must include Dedicated or shared intelligence analyst from OEM for continuous product usage support and regular reviews		
		Professional Service a) Full-time/ part-time “named” threat intelligence analyst services for threat intelligence operations support b) Daily/Weekly Alert Summary and Monthly Executive Summary Reports (if required) c) On-demand Analyst services for threat research and investigations and custom reports		
		Incident Response Services (a) On-demand Malware Analysis and Reverse Engineering Assistance (b) On-demand Computer Forensics Analysis, Log Analysis, and Investigation		

21.5.2.2. Specification for Threat Integration Platform

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
1	Threat Intel Sharing Platform Capabilities	To establish a comprehensive on premise Threat Intelligence Sharing Platform solution to consume threat intel information from commercial and OSINT threat intel sources including but not limited to CERT-In, NCIIPC etc and provide STIX/TAXII based URL output for consumption into OCAC owned and managed security devices such as NGFW, Web Proxy, IPS, AV, EDR, NDR, SIEM, SOAR, etc. .		
		The solution should be integrated with at least 2 OSINT feeds and 1 commercial feeds/risk lists(not in scope of TIP vendor) from day one. The commercial feed integration steps should be thoroughly documented both by the proposed \platform solution and by the commercial Threat Feed OEM on their respective websites or support portal/knowledgebase.		
		The proposed Threat Intelligence Sharing Platform must be a commercial Solution and should be modified to the extent of capabilities asked by OCAC as and when required during the duration of the project.		
		The offered solution must provide threat feed integration with Checkpoint and Fortinet make NGFW, Trend Micro make EDR/AV, McAfee Web Gateway and McAfee SIEM from day one (not limited to mentioned brands). Additional integration with other cyber security solution is in scope of bidder however bidder must factor min 30 man days for future customization and integrations.		
		The platform should support Threat Intelligence Collection, Evaluation, Ingestion, Processing, Translation, Prioritization, Integration &		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		Aggregation and real time Dissemination.		
		The platform should support machine readable threat intelligence sharing with no limit on the number of users and devices of OCAC. The solution must support sharing of intelligence, including atomic IOCs, URLs, CVE, hash values etc for consumption by security devices such as NGFW, Web Proxy, IPS, AV, EDR, NDR, SIEM, SOAR, etc.		
		The solution must support sharing of all types of threat entity supported, including commercial third-party bulletins, IOCs, events, campaigns, actors, and bulletins, signatures, with no loss in fidelity between the original document and the copy received by each stake holders		
		The solution must support out of the box integration with multiple external threat intelligence sources including but not limited to sources such as MISP / TAXII servers, industry-led (ISAC's), sectorial CERTs, Vendor /OEM CERTs, Government (CERTs) and other partners.		
		The solution must provide for creating and maintaining IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.		
		The solution should provide for automatic correlation to help finding relationships between attributes and indicators from malware, attacks campaigns or analysis. There should be provision to enable of disable Correlation on per event or per attribute basis.		
		The solution should provide for a flexible data model where complex objects can be expressed and linked together to express threat		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		intelligence, incidents or connected elements.		
		The solution must provide for an intuitive web interface accessible via common wed browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge and Safari.		
		The web interface must allow end-users to create, update and collaborate on events and attributes/indicators.		
		A graphical interface should allow for an option to navigate seamlessly between events and their correlations. An event graph functionality should also be provided to create and view relationships between objects and attributes.		
		The solution should provide for advanced filtering functionalities and warning list to help the analysts to contribute events and attributes.		
		The solution should provide options for analyst to collaborate on events and attributes to propose changes or updates to attributes/indicators.		
		The solution should have an out of box feed import capability to import and integrate any threat intel or OSINT feed from third parties. At least 2 OSINT feeds and 1 commercial feedsnot in scope of TIP vendor) should be integrated from day one for OCAC to provide feeds like C2 communicating IPs, weaponized domains, Log4Shell Potentially Malicious Scanners, Log4Shell Related Scanners, hash info of Recently Active Targeting Vulnerabilities in the Wild, CVE information which are Exploited in the Wild by Recently Active Malware, etc		
		The solution should have adjustable taxonomy to classify and tag events following custom classification schemes or existing taxonomies. The		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		solution should have a default set of well-known taxonomies and classification schemes to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organizations.		
		The solution must provide option to export the data in various formats such as IPS/IDS Formats (Suricata, Snort and Bro etc), OpenIOC, plain text, CSV, MISP XML and JSON output to integrate with other systems (network IDS, host IDS, custom tools)		
		The solution must provide for bulk-import, batch-import, free-text import, import from OpenIOC, STIX 2.0(or later), TAXII, ThreatConnect CSV or MISP format.		
		The solution must support import of human-generated structured data including XLS or CSV via the UI. The solution must support import of machine-generated structured data such as JSON or XML via an API		
		The solution must have integrated encryption and signing of the notifications via PGP and/or S/MIME depending of the user preferences.		
		The solution must support the import of threat intelligence that is stored locally and privately, without any storage in the SaaS service or any external system		
		The solution must support receipt, creation, and editing of STIX threat entities including -Campaigns, malware, Threat Actors, Incidents, Signatures, Reports, - ATT&CK TTPs and other threat entities supported by latest STIX standards.		
		The solution must be able to store at least 15 million IOCs including historical across a range of indicator Types, including IP Addresses [v4 & v6], Domains, URLs, File Hashes, email addresses.		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		The solution must be able to receive and store at least 5,000 events per second from a typical mix of event sources, with an efficient storage mechanism. The solution must be able to store the specified event and IOC volumes for a retention period of one year. The solution must be able to match newly-received IOCs against old events, and newly-received events against old IOCs, where 'old' is up to the one-year retention period. The solution must be able to identify new matches against historic data in near-real-time.		
		The solution must automatically de-duplicate threat intelligence. The solution must automatically detect and remove false positives		
		The solution must include applications to integrate and manage a data feed from the solution to a downstream SIEM. The solution must permit user-definable filters to determine which new intelligence is synchronized to the downstream security system, such as a minimum confidence score or a specific tag. The solution must be able to limit the number of IOCs sent to a control with limited capacity, and automatically prioritize the IOCs to be sent up to this limit.		
		The webUI must also have an option to search the commercial threat feed OEM directly regarding any IOC and get details like the risk score, related context etc without the need to visit the commercial OEM website.		
		The solution must allow the user to query an IOC and see all matching events and flows within the UI. The solution should allow the user to query an IOC tag and see all events and flows that match IOCs possessing that tag, within the UI.		

S.	Module	Requirement	Compliance (Yes/No)	Offered Parameter
		The solution should be able to provide context around relevant IOCs, such as whether a domain is a Dynamic DNS, on a shared hosting platform, a sinkhole, etc. The solution must be able to show all reporting sources for any given IOC, together with any context they provide such as tags, dates, and confidence scores. The solution must allow OCAC to utilize the it's API to integrate and / or automate data processing using scripts and/or other data stores.		
		The commercial and OSINT threat feeds once ingested into the solution must display vendor generated tags such as current risk score, severity level, OEM triggered risk rules etc		
		The solution must automatically 'age out' indicators in enterprise integrations. The solution should be able to provide a risk or threat score to assist in prioritization, based on the nature of the threat and the confidence of the indicator detected in the organization. The solution should support a wide range of integrated products 'out of the box', without the need of extensive custom development for integration, so as to provide a seamless on boarding experience for each member.		
2	Training	OEM should provide the training on usability of Platform		
3	Support	The solution must be provided with 24/7 access to the support team via web, email and phone		
		The solution must include Dedicated or shared intelligence analyst from OEM for continuous product usage support and regular reviews		

21.5.2.3.Specification for Web Application Scanning (WAS) Tool

S.No.	Minimum Technical Specifications	Compliance (Yes/No)	Offered Parameter
1	The proposed solution should support (DAST) dynamic application security testing. The proposed solution should provide as SaaS offering that is hosted from within India location data centers.		
2	The proposed solution should specify and explain the proposed licensing model for this solution (DAST) dynamic application security testing.		
3	The proposed solution should propose elastic asset licensing.		
4	The proposed solution should propose scanner deployment with the ability to deploy unlimited on-prem scanners at no additional cost.		
5	The proposed solution should be CVE compatible and provide at least 10 years of CVE coverage.		
6	The proposed solution should track: The Open Web Application Security Project (OWASP) Top 10 number, the Common Weakness Enumeration (CWE) number, and the Web Application Security Consortium (WASC) classification, as applicable.		
7	The proposed solution should propose free online on demand training curriculum/courses.		
8	The proposed solution must support multi-fqdn scanning.		
9	The proposed solution must allow users to scan their RESTful API endpoints by providing a Swagger or OpenAPI specification file.		
Architecture			
1	The proposed solution should propose unified Web App Scanning and Vulnerability Management.		
2	The proposed solution should be hosted on the cloud.		
3	The proposed solution should achieve SSAE16 SOC 2 and/or CSA Star certification.		
4	The proposed solution should propose cloud and on-prem scanners.		
5	The proposed solution should propose scanners that managed by the platform, e.g. updates to vulnerability signatures, code, and other updates.		
6	The proposed solution should provide a comprehensive API for automation of processes and integration with 3rd party applications .		
Authentication			

S.No.	Minimum Technical Specifications	Compliance (Yes/No)	Offered Parameter
1	The proposed solution should propose advanced authentication support, such as form based authentication, cookie-based authentication, NTLM support, and Selenium-based authentication, to address most web application requirements.		
2	The proposed solution should highlight and analyze vulnerabilities directly in the web app for quicker analysis.		
3	The proposed solution should support Google Chrome Extension to helps easily create and manage web application scans, including setting up authentication for web application scanning.		
4	The proposed solution should record authentication flows from within your browser to save time.		
Scanning			
1	The proposed solution should support multiple geographically distributed scanning engines managed by a central console.		
2	The proposed solution should be able to scan both internal and external web applications.		
3	The proposed solution should have options for a "quick scan" to get started, determine correct functioning, and so on, versus a deep full scan.		
4	The proposed solution should understand the customer Web Applications.		
5	The proposed solution should scan and Identify web application vulnerabilities - internally and externally facing.		
6	The proposed solution should propose a simple scan setup and management.		
7	The proposed solution should propose safe scanning of Web Applications.		
8	The proposed solution should scan all of applications, including those built using modern web frameworks, such as JavaScript, AJAX, HTML5 and Single Page Applications.		
9	The proposed solution should deliver highly accurate results with minimal false positives and negatives, giving you and your developers confidence that your reports are accurate.		
10	The proposed solution should propose automated Web Application Scanning.		
11	The proposed solution should rapidly detect cyber hygiene issues.		

S.No.	Minimum Technical Specifications	Compliance (Yes/No)	Offered Parameter
12	The proposed solution should have capabilities for human-assisted crawling of the application so the scanner can better understand authentication flow.		
13	The proposed solution should propose frequent and automated scans.		
14	The proposed solution should reduce product sprawl.		
15	The proposed solution should identify the relevant Web page and URL where the vulnerability was detected.		
16	The proposed solution should have options to reduce the risk that minimum disruptions to service are caused when testing/performed against production applications.		
17	The proposed solution should reduce manual work efforts.		
18	The proposed solution should propose a high-level scan that analyzes HTTP security headers and other externally-facing configurations on a web application to determine if the application is compliant with common security industry standards.		
19	The proposed solution should rapid security assessments.		
20	The proposed solution detect improperly issued or soon-to-expire SSL/TLS certificates		
21	The proposed solution should cover the OWASP Top 10 categories.		
22	The proposed solution should propose 3rd-party component scanning.		
23	The proposed solution should propse scan progress indicators: Percentage, Estimate, Progress Bar.		
24	The proposed solution should propose actionable remediation instructions in a language developers understand.		
Product Security			
1	The proposed solution should encrypt data at rest - data is stored on encrypted media using at least one level of AES-256 encryption.		
2	The proposed solution should encrypt data in transit - data is encrypted in transport using TLS v1.2 with a 4096-bit key (this includes internal transports)		
3	The proposed solution should encrypt sensor communication – Traffic from the sensors to the platform is always initiated by the sensor and is outbound-only over port 443. Traffic is encrypted via SSL communication using TLS 1.2 with a 4096-bit key.		

S.No.	Minimum Technical Specifications	Compliance (Yes/No)	Offered Parameter
4	The proposed solution should support Single sign-on (SSO) authentication methods.		
5	The proposed solution should support Two-Factor Authentication (2FA).		
6	The proposed solution should have disaster recovery procedures and redundancies in place to minimize disruption.		
7	The proposed solution should service strive to provide a 99.95% or better uptime.		
8	The proposed solution should be able to partition/segregate customer data from other users.		
9	The proposed solution should not access, store, or process any Personally Identifiable Information (PII) or Protected Health Information (PHI).		
10	The proposed solution should have all data in all states in the cloud platform is encrypted with at least one level of encryption, using no less than AES-256.		
Visibility and Reporting			
1	The proposed solution should include customizable graphical and list based dashboards elements for displaying vulnerabilities and status of the assessed environment.		
2	The proposed solution should propose unified modern attack surface visibility.		
3	The proposed solution should propose easily verify vulnerabilities with proof and output reporting.		
4	The proposed solution should propose the OWASP Top 10 categories report and dashboard.		
5	The proposed solution should support the ability to produce reports in the following report formats: Json, CSV, XML.		
6	License to be Provided No .of FQDNs- Minimum 1000 FQDNs		

21.5.2.4. Project Citation Format

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

NB:

Please attach supporting documents like Workorder , Completion Certificate Etc.

21.6. Form 5: Letter of Proposal

To,

The General Manager (Admn)
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
P.O.- RRL, Bhubaneswar - 751013
EPBX: 0674-2567280/2567064/2567295
Fax: +91-0674-2567842

Subject: Submission of the Bid Proposal for < Package – I / Package -II against RFP No >

Dear Sir/Madam,

We, the undersigned, hereby submit our Proposal against your Request for Proposal floated vide RFP Ref: OCAC-CERT-CYS-0001-2023-24035, Dated 28/02/2024, in a separate sealed envelope.

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

We undertake, if our Proposal is accepted, to initiate the Implementation services related to the assignment not later than the date indicated in Fact Sheet.

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 understand you are not bound to accept any Proposal you receive.

Yours sincerely,

Authorized Signature [*In full and initials*]: ______________________________

Name and Title of Signatory: ____

Name of Firm: ____

Address: ____

Location: ________________________Date: _________________

21.7. Form 6: Undertaking on Authenticity of IT Hardware / Software & peripherals

(To be filled by the bidder (On Rs. 100/- Non-judicial stamp paper)

To

The General Manager (Admn),
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
P.O. - RRL, Bhubaneswar - 751013
EPBX: 0674-2567280/2567064/2567295
Fax: +91-0674-2567842

Reference: OCAC-CERT-CYS-0001-2023-24035, Dated 28/02/2024,

This has reference to the items being supplied/ quoted to you vide our bid ref. no. : OCAC-CERT-CYS-0001-2023-24035, Dated 28/02/2024 under Package – I / Package - II

We hereby undertake that all the components/ parts/ assembly/ software / service used in the equipment shall be genuine, original and new components /parts/ assembly/ software from respective OEMs of the products and that no refurbished/ duplicate/ second hand components/ parts/ assembly/ software are being used or shall be used. In respect of licensed operating system, we undertake that the same shall be supplied along with the authorized license certificate with our name/logo. Also, that it shall be sourced from the authorized source for use in India.

In case, we are found not complying with above at the time of delivery or during installation, for the equipment already billed, we agree to take back the equipment already supplied at our cost and return any amount paid to us by you in this regard and that you will have the right to forfeit our EMD/PBG for this bid or debar/ black list us or take suitable action against us.

Authorized Signatory
Name:
Designation:

Note: The signing Authority should be not lower than Company Secretary of the OEM.

21.8. Appendix II: Commercial Proposal Templates

21.8.1. Form 7: Covering Letter

< Location, Date >

To,

The General Manager (Admn)
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
P.O.- RRL, Bhubaneswar - 751013
EPBX: 0674-2567280/2567064/2567295
Fax: +91-0674-2567842

Subject: Submission of the Financial bid for OCAC-CERT-CYS-0001-2023-24035, Dated 28/02/2024 Package – I / Package - II

Dear Sir/Madam,

We, the undersigned, hereby submit our Financial Proposal against your Request for Proposal floated vide RFP no OCAC-CERT-CYS-0001-2023-24035, Dated 28/02/2024 Package – I / Package – II.

Our attached Financial Proposal is for the sum of [*Amount in words and figures*] along with applicable taxes & duties.

Our Financial Proposal shall be binding upon us, up to expiry of the validity period of the Proposal, i.e., [*Date*].

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

We remain,

Yours sincerely,

Authorized Signature:

Name and Title of Signatory:

Name of Firm:

Address:

21.8.2. Form 8: Financial Proposal Package - I

Sl. No.	Item Description	Qty	Unit	Base Product Cost Including 5 Years OEM Support	Base Installationcost	Unit Price	GST Charges as applicable	Total Product Cost (Including GST)
1	2	3	4	5	6	7= 5+ 6	8	9= 7+8
1	Firewall (NGFW) in High Availability (HA) (Fully populated from day 1)	02	Nos					
2	L2 Network Switch 24Port (Fully Populated from day 1)	01	Nos					
3	Optical Patch Cable, OM4 Multi-mode mode,Duplex LC-LC,10 meters (Commscope / Panduit /Molex)	20	Nos.					
4	Optical Patch Cable, OM4 Multi-mode mode,Duplex SC-LC,10 meters (Commscope/Panduit/ Molex)	20	Nos.					
5	CAT6 UTP Patch Cord – Factory Crimped,3 meters(Commscope / Panduit /Molex)	20	Nos.					
6	CAT6 UTP Patch Cord –Factory Crimped,10 meters (Commscope/Panduit/ Molex)	10	Nos.					
7	Total							
Grand Total Cost (Amount quoted in words) : - Rupees								

Authorized Signatory with Official Seal

Signature & Seal of the Bidder

NOTE :-

- Prices shall be quoted inclusive of all taxes, duties, freight and forwarding and cost of labour for installation in Indian Rupees i.e INR
- Printed brochures of items quoted should be enclosed.
- The bidder should mention the warranty period against all manufacturing defects.
- In case of any discrepancy between Unit Price & Total Price, the Unit Price will prevail.

21.8.3. Form 9: Financial Proposal Package – II

A. Price Bid

SL. No.	Item	Quantity (a)	Unit Cost (in Rs.) (b)	Taxes (in Rs.) (c)	Total Cost (in Rs.) (d = b + c)	Total Amount (in Rs.) (e = a x d)
1.	Threat Intel Solution (Cost Should include all components asked in Technical Specification excluding Take Down Service)- Section 21.5.2.1	1				
2.	Threat Integration Platform- Section 21.5.2.2	1				
3.	Web Application Scanning Tool(cost should include the cost for Enterprise Licenses, integration with end user departments, updates, upgrades, dashboard configuration and support etc)- Section 21.5.2.3	1				
4.	Operation & Maintenance	1				
					Total Cost	
Grand Total Cost (Amount quoted in words) : - Rupees						

Authorized Signatory with Official Seal

- Prices shall be quoted inclusive of all taxes, duties, freight and forwarding and cost of labour for installation.
- OCAC reverse the right to issue the workorder for complete Package- II or Part worder for Solution asked for.
- Price shall include one time OEM Training / Certification cost for 4 resources of OCAC from OEM
- Training at the time of Installation, Configuration & Hand holing of tool should be free of cost and should be provided by OEM
- Price should be inclusive of 5 year Premium Service Support
- Printed brochures of items quoted should be enclosed.

- The bidder should mention the warranty period against all manufacturing defects.
- In case of any discrepancy between Unit Price & Total Price, the Unit Price will prevail.

B. Price Discovery

SL. No.	Item	Quantity (a)	Unit Cost (in Rs.) (b)	Taxes (in Rs.) (c)	Total Cost (in Rs.) (d = b + c)	Total Amount (in Rs.) (e = a x d)
1.	Threat Intel Solution- Take Down Service (As per Scope of Take Down Mentioned in Technical Specification of Threat Intel Solution) - Section 21.5.2.1	500				
					Total Cost	
Grand Total Cost (Amount quoted in words) : - Rupees						

Authorized Signatory with Official Seal

- For the take down services, Payment will be released as per actual consumption of number of successful takedowns at the end of every quarter. The bidder shall raise correct and clear invoice at the end of each quarter based on actual consumption.
- Work order will be issued excluding Take Down Service Feature, but the Feature should be available in the Solution without additional License Cost.
- The Bidder has to consider 500 Takedown for Entire duration of Contract
- The unit cost proposed should be valid for entire duration of Contract.

21.9. Appendix III: Templates

21.9.1. Form 10: Performance Bank Guarantee (PBG)

To,

The General Manager (Admn)
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
PO: - RRL, Bhubaneswar - 751013
EPBX: 0674-2567280/2567064/2567295
Fax: +91-0674-2567842

Whereas, << name of the supplier and address >>(hereinafter called "the Bidder") has undertaken, in pursuance of contract no. << insert contract no. >> dated. << insert date >> to provide Implementation services for << name of the assignment >> to OCAC (hereinafter called "the beneficiary")

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

And whereas we, << name of the bank >> a banking company incorporated and having its head /registered office at << address of the registered office >> and having one of its office at << address of the local office >>have agreed to give the supplier such a bank guarantee.

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

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

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

This Guarantee shall be valid until << *Insert Date* >>)

Notwithstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed Rs<< insert value >>(rupees << insert value in words >> only).

II. This bank guarantee shall be valid up to *<< insert expiry date >>*)

III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before *<< insert expiry date >>*) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)
Seal:
Date:

21.9.2. Form 12: Draft Agreement Format (subject to change as per requirement)

(To be signed by selected bidder(s) and tendering authority)

An agreement made this____(enter date of Agreement) between (enter your firm's name & address) (hereinafter called "the approved supplier", which expression shall, where the context so admits, be deemed to include his heirs, successors, executors and administrators of the one part and the OCAC which expression shall, where the context so admits, be deemed to include his successors in office and assigns of the other part.

Whereas the approved supplier has agreed with OCAC to supply to the General Manager (Admn.), Odisha Computer Application Centre, Plot No.-N-1/7-D, Po-RRL, Acharya Vihar, Bhubaneswar,Odisha-751013 all those articles set forth in our Work Order No. __________Dated ______ appended hereto in the manner set forth in the conditions of the bidding document and contract appended herewith and at the rates set forth in the said order.

And whereas the approved supplier has deposited a sum of Rs.______________in the form of:

a. Bank Draft No. / Banker Cheque / Bank Guarantee No.____________ dated. Valid up to ____________________.

Now these Presents witness:

1. In consideration of the payment to be made by OCAC through cheque/ DD at the rates set forth in the Work Order hereto appended the approved supplier will duly supply the said articles set forth in our Work Order No.______________________dated /______/20___thereof in the manner set forth in the Notice Inviting Tender (NIT), Tender Form, Instructions to Bidders, Terms of Reference, General and Special Conditions of the Tender and Contract, Technical Bid and Financial Bid along with their enclosures.
2. The Notice Inviting Tender(NIT), Tender Form, Scope of Work, General and Special Terms & Conditions of the Tender and Contract, Technical Bid and Financial Bid along with their enclosures enclosed with the Tender Notice No.: OCAC-XXXXXXXXXXXXXXXXXXX, Dated–XX/XX/2024 and also appended to this agreement will be deemed to be taken as part of this agreement and are binding on the parties executing this agreement.
3. Letter Nos.______________ dated _________ received from {bidder} and letter Nos.____________ Dated ___________ issued by OCAC and appended to this agreement shall also form part of this agreement.

4. OCAC do hereby agree that if the approved supplier shall duly supply the said articles in the manner aforesaid observe and keep the said terms and conditions, OCAC will through cheque/ DD pay or cause to be paid to the approved supplier at the time and the manner set forth in the said conditions, the amount payable for each and every consignment.
5. The mode of payment will be as specified in this bidding document/ work order.

   The prescribed scope of work/ requirement of services and deployment of technical resources shall be effected and completed within the period as specified in the Work Order. In case of extension in the delivery period/ completion period with liquidated damages, the recovery shall be made on the basis of following percentages of value of stores/ works which the bidder has failed to supply or complete the work.

No.	Condition
1	For delay in delivery of materials beyond the delivery schedule mentioned in the work order**, LD @ 0.5%** per week or part thereof for the pending materials order value up to maximum **5%** will be deducted.

a. The maximum amount of liquidated damages shall be **5%** of the desired Lot.
b. OCAC reserves its right to recover these amounts by any mode such as adjusting from any payments to be made by OCAC to the bidder.
c. If the supplier requires an extension of time in completion of contractual supply on account of occurrence of any hindrances, he shall apply in writing to the authority which had 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 goods on account of hindrances beyond the control of the bidder.

Warranty / Services shall be provided by the bidder as per terms and conditions of the RFP and Contract.

All disputes arising out of this agreement and all questions relating to the interpretation of this agreement shall be decided by OCAC and the decision of OCAC shall be final.

In witness whereof the parties hereto have set their hands on the ___ day of____ (Year)**.**

Signature of the Approved Supplier/ bidder

Designation:

Date:

Witness No.1

Witness No.2

Signature for and on behalf of OCAC

Designation:

Date:

Witness No.1

Witness No.2