RFP ENQUIRY No: OCAC-TE-17/2018(P-I)/ENQ-20030

CORRIGENDUM – Part 2

Last Date of Submission of Proposal:18-12-2020, 2:00 PM, Opening of General and Technical Bids on 18-12-2020, 3:30 PM

RFP ENQUIRY No: OCAC-TE-17/2018(P-I)/ENQ-20030, Date 24.09.2020 for selection of bidders for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre (CSOC).

Important : The Corrigendum-Part2 is to be read along with the Original RFP document published on the Website http://www.ocac.in & www.odisha.gov.in Vide RFP Enquiry number: OCAC-TE-17/2018(P-I)/ENQ-20030, Date 24.09.2020 and the Corrigendum published on Website http://www.ocac.in

<table>
<tr><th>Sr. No.</th><th>RFP / Corrigendum Clause No.</th><th>RFP / Corrigendum Page no.</th><th>Existing RFP / Corrigendum Clause Details</th><th>Modification / Remarks</th></tr>
<tr><td>1.</td><td>3.10.2 Technical evaluation
Sr. no. 6</td><td>23</td><td>Quality of the CVs of resources proposed for the CSOC project

The quality / scoring of CVs would be considered on basis of years of relevant experience, qualification, certification, projects associated with, etc. The process would be held under a technical panel of OCAC.

<table><tr><td>CV of resource proposed for SOC Manager</td><td>Maximum 02 mark</td></tr><tr><td>CV of resource proposed for Security administration and Threat Intelligence expert</td><td>Maximum 02 mark</td></tr><tr><td>CV of resources proposed for CSOC Engineer - 0.5 marks for each resource</td><td>Maximum 1.5 marks</td></tr><tr><td>CV of resources proposed for Level 2 analyst - 0.5 marks for each resource</td><td>Maximum 3.5 marks</td></tr><tr><td>CV of resources proposed for Level 1 analyst - 0.5 marks for each resource</td><td>Maximum 3.5 marks</td></tr></table></td><td>The clause should be read as:

Quality of resources proposed for the CSOC project.

The quality / scoring of resources would be considered on basis of interview, years of relevant experience, qualification, certification, projects associated with, etc. The process would be held under a technical panel of OCAC. The CVs must include the personnel who would be proposed for interview.

Interviews to be held through a technical panel of OCAC. The interview for all proposed personnel will be held collectively and not on individual basis.

The successful bidder has to deploy manpower at par with the caliber and knowledge of the interviewed manpower. In case the actual resources deployed are not found at par with the CVs or interviewed personnel, then the bidder has to deploy the resources who was interviewed by OCAC.

<table><tr><td>CV and interview of resource proposed for SOC Manager</td><td>Maximum 03 mark</td></tr></table></td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>RFP / Corrigendum Clause No.</th><th>RFP / Corrigendum Page no.</th><th>Existing RFP / Corrigendum Clause Details</th><th>Modification / Remarks</th></tr>
<tr><td></td><td></td><td></td><td></td><td>
<table>
<tr><td>CV and interview of resource proposed for Security administration and Threat Intelligence expert</td><td>Maximum 05 mark</td></tr>
<tr><td>CV of resources proposed for CSOC Engineer (03 personnel)

Interview of CSOC Engineer (at least one personnel)</td><td>Maximum 05 marks</td></tr>
<tr><td>CV of resources proposed for Level 2 analyst (07 personnel)

Interview of Level 2 analyst (at least 3 personnel)</td><td>Maximum 06 marks</td></tr>
<tr><td>CV of resources proposed for Level 1 analyst (07 personnel)

Interview of Level 1 analyst (at least 3 personnel)</td><td>Maximum 06 marks</td></tr>
</table>
</td></tr>
<tr><td>2.</td><td>3.10.2 Technical evaluation
Sr. no. 7</td><td>24</td><td>Quality of resources to be proposed for CSOC operations.

The quality / scoring of resources would be considered through interviews to be held through a technical panel of OCAC. The interview for CSOC Engineer, Level 1 analyst and Level 2 analyst will be held collectively and not on individual basis.</td><td>The point stands deleted</td></tr>
</table>

Sr. No.	RFP / Corrigendum Clause No.	RFP / Corrigendum Page no.	Existing RFP / Corrigendum Clause Details	Modification / Remarks
3.	3.10.2 Technical evaluation Sr. no. 8	24	Quality of technical design, approach methodology, solution specifications Technical presentation to be given by the bidder to OCAC. Marks would be awarded as per the technical committee of evaluation from OCAC. Marks would be distributed as per the approach and methodology, past experiences and credentials presented by the bidder. - 10 marks	The clause should be read as: Quality of technical design, approach methodology, solution specifications Technical presentation to be given by the bidder to OCAC. Marks would be awarded as per the technical committee of evaluation from OCAC. Marks would be distributed as per the approach and methodology, past experiences and credentials presented by the bidder. - 15 marks
4.	3.10.2 Technical evaluation Sr. no. 9	24	Quality of technical design, approach methodology, solution specifications Technical presentation to be given by the bidder to OCAC. Marks would be awarded as per the technical committee of evaluation from OCAC. Marks would be awarded as per superiority in terms of technical specifications and capacity of the solutions as proposed by the bidder. - 10 marks	The clause should be read as: Quality of technical design, approach methodology, solution specifications Technical presentation to be given by the bidder to OCAC. Marks would be awarded as per the technical committee of evaluation from OCAC. Marks would be awarded as per superiority in terms of technical specifications and capacity of the solutions as proposed by the bidder. - 15 marks
5.	Corrigendum: Addition to Section 14.1 General terms Point 2	Corrigendum Page 25	All data related to the Bug bounty activity would be on-premises, no data would be authorized to be taken outside OCAC premises.	The clause should be read as: The bidder may implement the Bug Bounty program on-premises or through cloud services. In case of cloud services, the bidder should comply as per MeitY, GoI guidelines and OCAC requirement. The cloud service provider (CSP) should be enlisted as Ministry of Electronics and Information Technology, Government of India empaneled CSP.

Sr. No.	RFP / Corrigendum Clause No.	RFP / Corrigendum Page no.	Existing RFP / Corrigendum Clause Details	Modification / Remarks
6.	Corrigendum: Addition to Section 14.1 General terms Point 4	Corrigendum Page 25	All hardware / solution as proposed by the bidder for the Bug bounty activity is to be hosted in Odisha State Data Centre (OSDC) or any location designated by OCAC.	The clause should be read as: The bidder may implement the Bug Bounty program on-premises or through cloud services. In case of cloud services, the bidder should comply as per MeitY, GoI guidelines and OCAC requirement. The cloud service provider (CSP) should be enlisted as Ministry of Electronics and Information Technology, Government of India empaneled CSP.
7.	Corrigendum: Addition to Section 14.1 General terms Point 7	Corrigendum Page 25	Under the authorization of OCAC, the bidder to coordinate with the respective department for the Bug bounty activity and environment establishment.	The clause should be read as: Under the authorization of OCAC, the bidder to coordinate with the respective department for the Bug bounty activity and environment establishment. Any clarification / justification required by the department or any personnel assigned by the department should be coordinated by bidder on-premises. Deployed SOC manpower should be capable for coordinating with the stakeholders for any clarification / justification regarding any vulnerability or bug reported by the bidder for any application / website through Bug Bounty activity.
8.	Corrigendum Point 4 3.10.1 Eligibility criteria Sr. No. 7	Corrigendum Page 2	The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.03.2020. SOC solution could be On-premises SOC / Managed SOC / Hybrid SOC. At least 3 government / PSU / Telecom / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5crore.	The clause should be read as: The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.06.2020. SOC solution could be On-premises SOC / Managed SOC / Hybrid SOC. At least 3 government / PSU / Telecom / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5 crore. SOC project which may be a part / portion of a project with large and various scope of work will be considered under the eligibility criteria, provided that: 1. The scope of SOC project (ongoing or completed) should be clearly segregated and mentioned in the WO / PO / Client satisfactory letter. 2. The value of the SOC project / SOC implementation should be clearly mentioned.

Sr. No.	RFP / Corrigendum Clause No.	RFP / Corrigendum Page no.	Existing RFP / Corrigendum Clause Details	Modification / Remarks
				3. Any number SOC project / SOC implementation which are a part of a larger project to be considered as a single SOC project only. SOC projects should comprise of implementation, operations and maintenance of more than one Cyber security products like SIEM, WAF, Anti-APT, UBA, NTA, NAC, SOAR, IR solution, etc.
9.	Corrigendum Point 7 3.10.2 Technical evaluation Sr. No. 1	Corrigendum Page 4	The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.06.2020. SOC solution could be On-premises SOC / Managed SOC / Hybrid SOC. At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5 crore. More than or equal to 8 Govt. / PSU / Telecom / BFSI clients. - 10 marks More than or equal to 5 and less than 8 Govt. / PSU / Telecom / BFSI clients. - 08 marks More than or equal to 3 and less than 5 Govt. / PSU / Telecom / / BFSI clients. - 07 marks	The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.06.2020. SOC solution could be On-premises SOC / Managed SOC / Hybrid SOC. At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5 crore. More than or equal to 8 Govt. / PSU / Telecom / BFSI clients. - 10 marks More than or equal to 5 and less than 8 Govt. / PSU / Telecom / BFSI clients. - 08 marks More than or equal to 3 and less than 5 Govt. / PSU / Telecom / / BFSI clients. - 07 marks SOC project which may be a part / portion of a project with large and various scope of work will be considered under the technical evaluation criteria, provided that: 1. The scope of SOC project (ongoing or completed) should be clearly segregated and mentioned in the WO / PO / Client satisfactory letter. 2. The value of the SOC project / SOC implementation should be clearly mentioned. 3. Any number SOC project / SOC implementation which are a part of a larger project to be considered as a single SOC project only. SOC projects should comprise of implementation, operations and maintenance of more than one Cyber security products like SIEM, WAF, Anti-APT, UBA, NTA, NAC, SOAR, IR solution, etc.

CLARIFICATION:

Sr. No.	RFP / Corrigendum Clause No.	RFP / Corrigendum Page no.	Existing RFP / Corrigendum Clause Details	Clarification
1.	3.10.2 Technical evaluation	22	Experience in implementation of on-premises Cyber Security operations centre.	On-premises SOC would be considered for projects where the SOC solutions and manpower both were deployed at the client premises and operations managed on-premises. Any project where the solution was deployed on-premises but operations management was done remotely would be considered as Managed SOC rather than On-premises SOC. SOC projects should comprise of implementation, operations and maintenance of more than one Cyber security products like SIEM, WAF, Anti-APT, UBA, NTA, NAC, SOAR, IR solution, etc.