CORRIGENDUM

Last Date of Submission of Proposal:04-12-2020, 2:00 PM, Opening of General and Technical Bids on 04-12-2020, 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 is to be read along with Response Sheet published with this corrigendum and 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

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
1.	1. Introduction to Cyber Security Operation Centre (CSOC).	8	In recent times organizations are shifting their focus more on the human element than the technology element to assess and mitigate threats directly rather than rely on a script. While technology systems such as Firewall, IPS or other security appliances may prevent basic attacks, human analysis is required to put major incidents to rest.	Bug Bounty is added as a scope of work for bidder. Details provided below in the document.
2.	3.5 General Instructions to bidders	15	The bidder may propose "Make in India" products and solutions in their bid, however the products / solutions should be in compliance with the required guidelines and standards. They should also meet the criteria and minimum requirement as mentioned in the RFP document.	The bidder may propose "Make in India" products and solutions in their bid, however the products / solutions should be in compliance with the required guidelines and standards and MeitY notification dated 6th December, 2019 "Public procurement (preference to Make in India) order 2019 for Cyber Security products". They should also meet the criteria and minimum requirement as mentioned in the RFP document.

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
3.	3.5 General Instructions to bidders	16	Consortium or subcontracting of any kind shall not be acceptable for this project. Any deviation would lead to disqualification or termination of the same. However, as per the State ICT Policy 2014 clause 5.5.2, it is mandated that the successful bidder must associate a local enterprise, who has not been debarred / blacklisted by state Government. The involvement / association of the local enterprise is limited to maximum 25% of the total project. The work allotted to the local enterprise may be limited to any one of the following: i. Civil and interior works of the SOC sites. ii. Installation, maintenance and support of the Non-IT items for SOC. Iii. Manpower deployed for SOC. The local enterprise should have relevant experience, expertise and reach in the associated scope of work or activity. The successful bidder has to submit scope of work, credential and experience details of the local enterprise with OCAC.	The modified clause to be read as: Consortium of any kind shall not be acceptable for this project. Any deviation would lead to disqualification or termination of the same. However, as per the State ICT Policy 2014 clause 5.5.2, it is mandated that the successful bidder must associate a local enterprise which is limited to maximum 25% of the of the project for deployment and maintenance components. The successful bidder shall make collaborative arrangements for implementation with local enterprises having relevant experience and reach. Any subcontracting other than the scope mentioned above is not permitted under the project. The local enterprise should have relevant experience, expertise and reach in the associated scope of work or activity. The successful bidder shall submit scope of work, credential, experience and registration details of the local enterprise with OCAC.
4.	3.10.1 Eligibility criteria Sr. No. 7	20	The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.12.2019. SOC solution could be On-premises SOC, Managed SOC, Hybrid SOC. At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5crore.	The modified clause to be read as: 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.

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
5.	3.10.1 Eligibility criteria; Sr No: 5	20	The bidder should have a minimum average annual turnover of at least Rs. 200 Crores in the last three financial years (i.e. 2016-17, 2017-18 & 2018-19).	The modified clause to be read as: " The bidder should have a minimum average annual turnover of at least Rs. 200 Crores in the last three financial years (i.e. 2017-18, 2018-19 & 2019-20). In case the bidder does not have the audit financial statements then a letter in the head of the chartered accountant / or firm certifying the financial turnover of the company is to be submitted with the bid. In case the bidder faces challenge in the letter submission, then bidder may submit the audited financial statements for financial years (i.e. 2016-17, 2017-18 & 2018-19)."
6.	3.10.1 Eligibility criteria, Sr.no.11	21	The bidder should be: · ISO 9001:2008 or later certified · ISO 20000: 2018 certified · ISO 27001: 2013 certified	The modified clause to be read as: The bidder should be: · ISO 9001:2008 or later certified · ISO 20000: 2011 or later certified · ISO 27001: 2013 or later certified

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
7.	3.10.2 Technical evaluation Sr. No. 1	22	The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.12.2019. SOC solution could be On- premises SOC, Managed SOC, Hybrid SOC. At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5 crore. More than or equal to 8 Govt. / BFSI clients. - 10 marks More than or equal to 5 and less than 8 govt. / BFSI clients. - 07 marks More than or equal to 3 and less than 5 govt. / BFSI clients. - 05 marks	The modified clause to be read as: 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 / 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

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
8.	3.10.2 Technical evaluation Sr. no. 5	23	Certified CISA, CEH, CISSP, CISM, CRISC, or equivalent (any one) personnel under the payroll of the company	The modified clause to be read as: Certified CISA, CEH, CISSP, CISM, CRISC, or equivalent (any one) personnel under the payroll of the company An undertaking in the company's letter head signed by authorized signatory to be submitted. The undertaking should mention the name and employee code of the personnel along with certification. At least 04 CISSP, 05 CISA / CISM, 10 CEH and 06 SIEM solution certified personnel and 10 personnel any one certification mentioned. Total 35 personnel. - 10 marks At least 02 CISSP, 03 CISA /CISM, 05 CEH and 05 SIEM solution certified personnel and 10 personnel any one certification mentioned. Total 25 personnel. - 8 marks At least 03 CEH and 02 proposed SIEM solution certified personnel and 10 personnel any one certification mentioned. Total 15 personnel. - 5 marks

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
9.	3.10.2 Technical evaluation Sr. no. 6 &7	24	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. 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	The modified clause to be read as: 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. The interview would be for sample manpower. The successful bidder has to deploy manpower at par with the caliber and knowledge of the interviewed manpower. Interview of SOC Manager - maximum 02 marks Interview of Security administration and Threat Intelligence expert / SME - maximum 02 marks Interview of CSOC Engineer - maximum 4.5 marks Interview of Level 2 analyst (atleast 3 manpower) - maximum 7 marks Interview of Level 1 analyst (atleast 3 manpower) - maximum 7 marks 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. The CVs to be submitted may be on sample basis but should match the count of the resources proposed for the project. CV of SOC Manager - maximum 02 marks CV of Security administration and Threat Intelligence expert / SME - maximum 02 marks CV of resources for CSOC Engineer - 0.5 marks for each resource - Maximum 1.5 marks CV of resources for Level 2 analyst - 0.5 marks foreach resource - Maximum 3.5 marks

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
				CV of resources proposed for Level 1 analyst - 0.5 marks for each resource - Maximum 3.5 marks The CVs submitted and the interview of the resources is to be considered as tentative only. The CVs must include the personnel who would be proposed for interview. Incase the actual resources deployed are not found at par with the CVs or interview personnel, then the bidder has to deploy the resources whose CVs or interview was shared with OCAC.
10.	5.4 Site Civil & Non-IT works	41	Bidder should submit the below certificates / documents after the completion of control desk / console: a) ANSI / BIFMA Certificate for Consoles b) ISO 9001, ISO 14001 & OHSAS 18001 Certificate c) Green Guard Certificate for low emissions d) ROHS Compliance e) ASTM E84	The modified clause to be read as: Bidder should submit the below certificates / documents after the completion of control desk / console: a) ANSI / BIFM Certificate for Consoles OR b) ISO 9001, ISO 14001 & OHSAS 18001 Certificate OR c) Green Guard Certificate for low emissions d) ROHS Compliance e) ASTM E84

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
11.	5.4 Site Civil & Non-IT works	42	5. Command centre chair / Meeting room chair / Visitor Chair / Manager chair Command centre chair must ergonomically designed in such a manner that long hour seating does not become tiring. The preferred requirement of chair are: Mid Back Chair, for Manager High back, Mesh Back & Silver Epoxy Backbone, Synchronized Mechanism,4-Way Adjustable Armrest, Seat height adjustment, Standard 5-prong P/Nylon Base, BIFMA & GREEN GUARD certified.	The modified clause to be read as: 5. Command centre chair / Meeting room chair / Visitor Chair / Manager chair Command centre chair must ergonomically designed in such a manner that long hour seating does not become tiring. The preferred requirement of chair are: Mid Back Chair, for Manager High back, Mesh Back & Silver Epoxy Backbone, Synchronized Mechanism,4-Way Adjustable Armrest, Seat height adjustment, Standard 5-prong P/Nylon Base, BIFM & GREEN GUARD or OHSAS certified.
12.	6.2 UPS	46	UPS- Output power: Single phase 230V +/- 1% sinewave 50 Hz & Minimum output voltage of 400volt	The modified clause to be read as: Output power: Three phase 400V +/-1% sinewave 50 Hz
13.	6.2 UPS	46	The type of battery shall be VRLA batteries with combination of LMO & NMC (Lithium Manganese Oxide & Nickel, Manganese, and Cobalt).	The modified clause to be read as: "The type of battery shall be either VRLA batteries or combination of LMO & NMC (Lithium Manganese Oxide & Nickel, Manganese, and Cobalt)."
14.	6.3 Closed circuit television (CCTV) – POE Switch	47	Supports PoE Power up to 25 Watts for each PoE port	The modified clause to be read as: "Supports PoE Power up to 25 Watts for each PoE port for all ports"
15.	6.9 Display – Video wall with controllers and speakers / Functionality /Video wall	52	The Rear Projection Modules must be based on Single Chip DLP, Full HD (1920X1080) Native, Rear Projection technology. The displays shall utilize RGB Laser having different laser bank for different colors respectively without any moving part.	The modified clause to be read as: "The Rear Projection Modules must be based on Single Chip DLP, Full HD (1920X1080) Native, Rear Projection technology video wall."

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
16.	6.9 Display – Video wall with controllers and speakers / Functionality /Video wall	52	No moving Part like color wheel or Phosphor wheel should be present as moving parts has more failure tendency	The point stands deleted.
17.	6.9 Display – Video wall with controllers and speakers / Functionality /Video wall	52	Separate hardware server for monitoring features Wall or Panel On/Off, Brightness and Color, Input control, health monitoring.	The modified clause to be read as: "Hardware server for monitoring features Wall or Panel On/Off, Brightness and Color, Input control, health monitoring."
18.	6.9 Display – Video wall with controllers and speakers / Functionality /Video wall	52	Projector should in-built green color indicator when projector is in idle state.	The modified clause to be read as: "Please change this to Projection engine should have indicator when engine is in idle state."
19.	6.9 Display – Video wall with controllers and speakers / Technical Specifications/Video wall	55	Color repetition speed must be 18X Frame Rate or higher with 3 x 12-bit color and Brightness correction	The point stands deleted.
20.	6.9 Display – Video wall with controllers and speakers / Technical Specifications/Video wall	55	Redundant Power Supply External remote one to be provided only. This should be kept in the rack so that power supply can be changed without disturbing any cube or alignment.	The modified clause to be read as: "Dual redundant power supply for the videowall"
21.	6.9 Display – Video wall with controllers and speakers / Technical Specifications/Video wall	55	Each display module shall have minimum Redundant DP1.2 and HDMI 1.4 (HDCP compliant), DVI-DL inputs for redundancy purposes.	The modified clause to be read as: " Each display module shall have minimum Redundant DP1.2 and HDMI 1.4 (HDCP compliant), DVI-DL/ HDMI 2.0 or DVI/DP inputs"
22.	6.9 Display – Video wall with controllers and speakers / Technical Specifications/Video wall	55	Projector should capable of gen-lock 49 Hz - 61 Hz; 92 -120 Hz, also supports double genlock	The point stands deleted.
23.	6.9 Display – Video wall with controllers and speakers / Technical Specifications/ Controller	55	Input : H.264, MPEG2/4, MxPEG, MJPEG, V2D, H.263	The modified clause to be read as: "V2D input may considered optional"

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
24.	6.9 Display – Video wall with controllers and speakers / Technical Specifications/ Controller	55	Output : DP/DVI/HDMI, Outputs - Up to 48 HD displays	The modified clause to be read as: "Output : DP/DVI/HDMI, Outputs - Up to 12 HD displays"
25.	6.9 Display – Video wall with controllers and speakers / Technical Specifications/ Controller	55	Contrast ratio should be Min 1800 Lumens	The modified clause to be read as: "Contrast ratio to be 1800:1"
26.	6.10 Network Rack Sr. No. 16	56	Should be UL Listed and conform to EIA-310 Standard or India equivalent for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard x	The modified clause to be read as: "Should be UL Listed and conform to EIA-310 Standard or India equivalent for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard"
27.	7.1 Minimum technical requirement Security Orchestration Automation & Response (SOAR) Sr. No. 6	57	Should be able to automatically extract email attachments from emails and store that for the related incidents as attachments.	The point stands deleted.
28.	7.1 Security Orchestration Automation & Response (SOAR) Sr. No. 7	57	Solution should include 100+ out-of-the-box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DOS and DDOS attack, Phishing Attack, etc. and should support creation of multiple playbook.	The modified clause to be read as: "Solution should include out-of-the-box 100+ unique playbooks for incidents similar to Ransomware Attack, Data Leakage, Malware Attack, DOS and DDOS attack, Phishing Attack, etc. and should support creation of more than 100+ playbooks up to 400 unique playbooks (as per requirements) without any additional cost within the span of the project.". Ideally at least 100 additional playbooks should be created in each year.
29.	7.1 Minimum technical requirement Security Orchestration Automation & Response (SOAR) Sr. No. 25	58	Should have threat intelligence feeds to properly correlate to the end of discovering attack patterns, potential vulnerabilities and other ongoing risks to the organization.	The point stands deleted.

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
30.	7.1 Minimum technical requirement Security Orchestration Automation & Response (SOAR) Sr. No. 35	58	Should support recreation of any incident for simulation and analysis purpose.	The modified clause to be read as: "Should support recreation of any incident for analysis purpose."
31.	7.1 Security Orchestration Automation & Response (SOAR) Sr. No. 38	59	Solution should not have any restriction on the number of response actions and creation of playbooks.	The modified clause to be read as: "Solution should have capability for at least 1000 number of response actions per day. "
32.	7.1 Security Orchestration Automation & Response (SOAR) Sr. No. 43	59	Should have at least 150 out of the box API based integrations and additional integrations should be free.	The modified clause to be read as: "Should have at least 150 out of the box API based integrations and all additional integrations should be free of cost"
33.	7.3 Security Information and Event Management (SIEM) Sr. No. 1	61	The OEM of the solution should be in the Gartner, Forrester, IDC, NSS, etc. leader quadrant in any of the last three years.	The modified clause to be read as: "The OEM of the solution should be in the Gartner / Forrester / IDC / NSS, etc. leader quadrant in any of the last three years."
34.	7.4 Anti – Advanced Threat Persistent (Anti – APT) Sr. No.1	63	The OEM of the solution should be in the Gartner, Forrester, IDC, NSS, etc. leader quadrant in the latest reports.	The modified clause to be read as: "The OEM of the solution should be in the Gartner / Forrester / IDC / NSS, etc. leader quadrant in the latest reports."
35.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No.2	63	Lock down patient zero, stop the spread, and neutralize the attack at the initial point of infection before it spreads laterally.	The point stands deleted.
36.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No.6	63	Solution should have capabilities to configure files, IP, URLs and Domains to Blacklist or white list.	The modified clause to be read as: "Solution should have capabilities to configure IP, URLs and Domains to Blacklist or white list."

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
37.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No.9	63	Should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a dashboard	The modified clause to be read as: "Should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families where ever applicable through a dashboard"
38.	7.4 Anti – Advanced Threat Persistent (Anti – APT) Sr. No.11	63	The solution should be OS agnostic and should deploy static/dynamic analysis for emulation of threats on various operating systems like Windows, MAC, Linux, etc. irrespective of the versions. The solution should support Windows 7, Windows 8, Windows 10 Microsoft 2003, Microsoft 2008, Microsoft 2012, and Microsoft 2016 operating environments for Sandboxing, this requirement should be based on virtual execution and should not be Hardware or chip based function.	The modified clause to be read as: "The solution should be OS agnostic and should deploy static/dynamic analysis for emulation of threats on various operating systems irrespective of the versions. The solution should support Windows 7, Windows 8, Windows 10 Microsoft 2003, Microsoft 2008, Microsoft 2012, and Microsoft 2016 operating environments for Sandboxing, this requirement should be based on virtual execution and should not be Hardware or chip-based function."
39.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No.19	64	Capable of combining global telemetry from one of the world's largest cyber intelligence networks, with local customer context, to uncover attacks that would otherwise evade detection	The point stands deleted.
40.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No. 23	64	Able to monitor the instruction flow at the CPU-level to detect exploits attempting to bypass OS security controls	The point stands deleted.
41.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No. 26	64	Blocks deceptive phishing sites and alerts on password reuse	The modified clause to be read as: "Blocks deceptive phishing sites and generate alerts"

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
42.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No. 34	64	The proposed solution should support at least 100+ protocols (e.g. HTTP, FTP, SMTP, SNMP, IM, IRC, DNS and P2P protocols SMB, Database protocol MySQL, MSSQL, Microsoft Office, Visual Basic, Acrobat PDF, MAC OS X *.app, zip, tar, flash, executables, link libraries, etc.) for inspection and should block suspicious communications of zero day malware detected IP, URL and file.	The modified clause to be read as: "The proposed solution should support at least 100+ protocols / filetypes (e.g. HTTP, FTP, SMTP, SNMP, IM, IRC, DNS and P2P protocols SMB, Database protocol MySQL, MSSQL, Microsoft Office, Visual Basic, Acrobat PDF, MAC OS X *.app, zip, tar, flash, executables, link libraries, etc.) for inspection and should block suspicious communications of zero day malware detected IP, URL and file."
43.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. no. 43	65	In case there is no antivirus signature available for malware, solution should have the ability to exfiltrate data about the malware and share it with the antivirus solution providers.	The point stands deleted.
44.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No.55	65	The solution should support Windows XP, Windows 7, Windows 8, Windows 10 Microsoft 2003, Microsoft 2008, Solaris10, Redhat 5 & above Linux operating environments for Sandboxing, this requirement should be based on virtual execution and should not be Hardware or chip based function.	The read as same as: 7.4 Anti – Advanced Persistent Threat (Anti – APT) Sr. No.11
45.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No.58	65	The solution should support windows XP, Windows 7, Windows 8, windows 10 Microsoft 2003, Microsoft 2008 (32 bit & 64 bit OS), Solaris10, and RedHat 5 & above Linux operating environments for Sandbox file analysis. Solution should have option to upload custom sandbox image running in client's environment.	The read as same as: 7.4 Anti – Advanced Persistent Threat (Anti – APT) Sr. No.11
46.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No.61	66	Capable of performing multiple sandboxing environment in parallel, handling more than 50 virtual machines.	The modified clause to be read as: "Capable of performing multiple sandboxing environment in parallel, handling more than 40 virtual machines."

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
47.	7.4 Anti – Advanced Threat Persistent (Anti – APT) Sr. No. 62	66	Capable of processing more than 4000 unique files per hour and have provision for expansion whenever required	The point stands deleted.
48.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No.63	66	Supports OS: Win 10 (64-bit), Win 8.1 (64-bit), Win 8 (32-bit/64- bit), Win 7 (32-bit/64-bit), Win XP (32-bit/64-bit), Win Server 2016, Win Server 2012, Win Server 2012 R2, Win Server 2008, Win Server 2003, Android, Mac, Linux	The read as same as: 7.4 Anti – Advanced Persistent Threat (Anti – APT) Sr. No.11
49.	7.4 Anti - Advanced Persistent Threat (Anti-APT) Sr. No.64	66	Capable of generating reports in the following formats: STIX, OpenIOC, XML, JSON, HTML, PDF, text	The modified clause to be read as: "Capable of generating reports in the following formats: XML, JSON, HTML, PDF, text"
50.	7.5 Network Traffic Analyzer Sr. No. 18	67	Should be capable of bulk decryption of SSH, IPSec, HTTPS, SMTPS, IMAPS, SSL, TLS, etc. encrypted traffic for analysis and monitoring.	The modified clause to be read as: "Should be capable of decryption of SSH, IPSec, HTTPS, SMTPS, IMAPS, SSL, TLS, etc. encrypted traffic for analysis and monitoring."
51.	7.5 Network Traffic Analyzer Sr. No. 34	67	Operating system should be security hardened and embedded with overlaying kernel for high speed packet processing.	The modified clause to be read as: "Operating system should be security hardened and embedded with kernel for high speed packet processing."
52.	7.5 Network Traffic Analyzer Sr. No. 37	67	Monitor network traffic through SNMP, Netflow, WMI, Rest APIs, etc. and network sniffing.	The modified clause to be read as: "Monitor network traffic through Netflow, Rest APIs, etc. and network sniffing."
53.	7.6 Threat Intelligence feeds	68	Threat Intelligence feed has to be unique. This has to be from a different OEM and not the same as of SIEM / SOAR OEM to adhere to the dual incident monitoring design principle.	The modified clause to be read as: "Threat Intelligence feed has to be unique and adhere to the dual incident monitoring design principle. Threat Intelligence feed from OEM other than the SIEM / SOAR OEMs is preferable and would have added advantage in technical evaluation."
54.	7.7 Network Management Switch for Data centre Sr. No.12	69	Supports Layer 3 protocols: PIM-SM & SSM & DM, IS-IS, IS-ISv6	The modified clause to be read as: "Supports Layer 3 protocols: PIM-SM & SSM & DM, IS-IS or IS-ISv6"

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
55.	7.7 Network Management Switch for Data centre Sr. No.13	69	Supports Layer 3 protocols: VXLAN, VRRP, DCBX	The modified clause to be read as: "Supports Layer 3 protocols: VXLAN, VRRP, or equivalent"
56.	7.7 Network Management Switch for Data centre Sr. No.14	69	Supports Layer 3 protocols: 802,1Qbb, 802,1Qaz, FCoE, etc.	The modified clause to be read as: "Supports Layer 3 protocols: 802,1Qbb, 802,1Qaz, etc."
57.	7.7 Network Management Switch for Data centre Sr. No.20	69	Support management protocols: Hitless patch upgrades, IP management, Openflow, etc.	The modified clause to be read as: "Support management protocols: Hitless patch upgrades, IP management, Openflow, etc. or equivalent"
58.	7.7 Network Management Switch for Data centre Sr. No.26	69	Should have minimum MAC address table size of 128K	The modified clause to be read as: "Should have minimum MAC address table size of 50K"
59.	7.7 Network Management Switch for Data centre Sr. No.27	69	Should be capable of configuring more than 500 IPV4 and 5000 IPV6 routing	The modified clause to be read as: "Should be capable of configuring more than 5000 IPV4 and 5000 IPV6 routing"
60.	7.8 Network Router for SOC Command Centre Sr. No.2	69	Command-line interface (CLI), alarm, network management, logging, statistics aggregation, and on-board failure logging (OBFL).	The modified clause to be read as: "Command-line interface (CLI), alarm, network management, logging, statistics aggregation, etc."
61.	7.8 Network Router for SOC Command Centre Sr. no. 10	70	Should support Open Shortest Path First (OSPF), Enhanced IGRP(EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector,	The modified clause to be read as: "Should support Open Shortest Path First (OSPF) / Enhanced IGRP(EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector"
62.	7.8 Network Router for SOC Command Centre Sr. no. 12	70	Should support Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), RSVP, CDP, ERSPAN,IPSLA, Call Home, EEM, IKE, ACL, EVC, DHCP, FR, DNS, LISP,OTV[6], HSRP, RADIUS, AAA, AVC, Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast	The modified clause to be read as: "Should support Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), RSVP, IPSLA/equivalent, IKE, ACL, EVC/SVC, DHCP, FR, DNS, RADIUS, AAA, IPv4-to-IPv6 Multicast or equivalent"

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
63.	7.8 Network Router for SOC Command Centre Sr. no. 14	70	Should support Bidirectional Forwarding Detection (BFD), IEEE802.1ag, and IEEE802.3ah	The modified clause to be read as: "Should support Bidirectional Forwarding Detection (BFD), IEEE802.1ag or IEEE802.3ah"
64.	7.8 Network Router for SOC Command Centre Sr. no. 18	70	Should support Serial (RS-449, X.21, V.35, and EIA-530)	The modified clause to be read as: "Should support Serial (RS-449 / X.21 / V.35 / EIA-530)"
65.	7.8 Network Router for SOC Command Centre Sr. no. 26	70	Modular QoS CLI (MQC) policies on VLANs or tunnels	This point stands deleted.
66.	7.8 Network Router for SOC Command Centre Sr. no. 28	70	RJ-45 console ports and auxiliary ports, and a mini USB console port.	RJ-45 console ports and a mini USB console port.
67.	7.8 Network Router for SOC Command Centre Sr. no. 30	70	Two USB 2.0 ports for USB flash sticks or USB secure tokens (secure key distribution).	This point stands deleted.
68.	7.8 Network Router for SOC Command Centre Sr. no. 34	71	One RJ-45/RS-232 compatible auxiliary port	This point stands deleted.
69.	7.9 Managed Switch for SOC Command centre Sr. no 19	71	Should support security features: IP Source Guar, Dynamic ARP inspection	The modified clause to be read as: "Should support security features: IP Source Guard, Dynamic ARP inspection"
70.	7.9 Managed Switch for SOC Command centre Sr. no 30	72	Managed Switch: Should have minimum 48 x 10/100 Base TX ports and 4 x 100/1000 SFP/SFP+ ports.	The modified clause to be read as: "Managed Switch: Should have minimum 48 x 10/100/1000 Base TX ports and 4 x 1/10G SFP/SFP+ ports"
71.	7.9 Managed Switch for SOC Command centre Sr. no 32	72	Should have minimum switching capacity of 15 Gbps	The modified clause to be read as: "Should have minimum switching capacity of 150 Gbps"
72.	7.10 SAN Storage	73	Should support FC, iSCI protocols. BIS compliant and registered.	The modified clause to be read as: "Should support FC / iSCI protocols. BIS compliant and registered."
73.	7.11 Vulnerability Management Solution Sr. No.1	73	Vulnerability assessment solution The OEM of the solution should be in the Gartner, Forrester, IDC, NSS, etc. leader quadrant in the latest reports	The modified clause to be read as: "Vulnerability assessment solution The OEM of the solution should be in the Gartner / Forrester / IDC / NSS, etc. leader quadrant in the latest reports"

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
74.	7.12 Network Monitoring, Helpdesk and Ticketing tool Sr. no.3	75	NMS OEM must be an industry standard solution and shall be in the present for NPMD and ITSM both in latest published Gartner's MQ reports and leading analysts' reports like IDC or Forrester	The modified clause to be read as: "NMS OEM must be an industry standard solution and shall be in the present for NPMD and ITSM both in latest published Gartner's MQ reports or similar leading analysts' reports like IDC or Forrester, etc."
75.	8.2 Manpower qualification L2 Analyst	80	• B.E. / B-Tech / MCA • Total 6 Years of experience out of which, minimum 4 years of experience in SOC services conducting security device administration & management and minimum 2 years in SIEM tool & other security tools. • Certification in at least one industry leading SIEM product. • Certifications in security, such as CISA, CEH, CISSP, CISM, CRISC (any one) preferred. • Certification in ISO 27001:2013 or later version.	The modified clause to be read as: Level 2 Analyst • B.E. / B-Tech / MCA • Total 6 Years of experience out of which, minimum 4 years of experience in SOC services conducting security device administration & management and minimum 2 years in SIEM tool & other security tools. • Certification in at least one industry leading SIEM product. • Certifications in security, such as CISA, CEH, CISSP, CISM, CRISC (any one) preferred OR Certification in ISO 27001:2013 or later version.
76.	8.2 Manpower qualification, CSOC Engineer	80	Qualification required: • B.E / B-Tech / MCA / Diploma in relevant field. • Minimum of 3 years of experience in security device administration & management. • Have experience in vendor management, patch management, Helpdesk and incident management. • Certified in ITIL v3 or later version. • ISO 27001:2013 or later version certification preferred.	The modified clause to be read as: CSOC Engineer • B.E / B-Tech / MCA / Diploma in relevant field. • Minimum of 3 years of experience in security device administration & management. • Have experience in vendor management, patch management, Helpdesk and incident management. • Certified in ITIL v3 or later version or ISO 27001:2013 or later version certification preferred."
77.	8.2 Manpower qualification Security Administration and Threat Intelligence	80	• B.E / B-Tech/MCA • Minimum 8 years of experience out of which, minimum 5 years relevant experience in SOC services, SOC administration, threat analysis and hunting, SOC configuration and management.	The modified clause to be read as: Security Administration and Threat Intelligence expert • B.E / B-Tech/MCA • Minimum 8 years of experience out of which, minimum 5 years relevant experience in SOC services, SOC administration, threat analysis and hunting, SOC

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
			• Certification in security CISA, CEH, CISSP, CISM, CRISC (any one). • Certification in ISO 27001:2013 or later version. • Certification in CTIA from a recognized body is preferable.	configuration and management. • Certification in security CISA, CEH, CISSP, CISM, CRISC (any one) OR Certification in ISO 27001:2013 or later version preferable. • Certification in CTIA from a recognized body is preferable.
78.	11. Payment terms	96	Supply of all Non-IT asset. (excluding the civil and interior works) 20% of quoted cost by the bidder for Non- IT items (excluding the civil and interior works)	The modified clause to be read as: Payment would be released to the bidder only after the Installation and Commissioning of the assets.
79.	11. Payment terms	97	Installation and Commissioning & Testing of all Non-IT asset. (excluding the civil and interior works) 60% of quoted cost by the bidder for Non- IT items (excluding the civil and interior works)	The modified clause to be read as: Installation and Commissioning & Testing of all Non-IT asset. (excluding the civil and interior works) 80% of quoted cost by the bidder for Non- IT items (excluding the civil and interior works)
80.	11. Payment terms	97	Supply of all IT asset.	The modified clause to be read as: Payment would be released to the bidder only after the Installation and Commissioning of the assets.
81.	11. Payment terms	97	Installation and Commissioning of all IT asset. 60% of the quoted cost by the bidder for IT items	The modified clause to be read as: Installation and Commissioning of all IT asset. 80% of the quoted cost by the bidder for IT items
82.	11. Payment terms	97	Project Sign-Off & FAT (Go-Live of the Project) 10% of quoted CAPEX cost	The modified clause to be read as: Project Sign-Off & FAT (Go-Live of the Project) 20% of quoted CAPEX cost
83.	11. Payment terms	97	Completion of one year of O&M phase 10% of quoted CAPEX cost	This point stands deleted.
84.	11.1.1 Supply, Installation, Commissioning	100	Submission of PBG-Within 30 days of LOI / Award to contract to successful bidder	The modified clause to be read as: "Submission of PBG-Within 30 days of LOI / Award to contract to successful bidder, whichever is later. Penalty on the delay of submission of PBG has been exempted"

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
85.	11.1.3 Manpower	106	Penalty for Substitution of Resources from those whose CVs provided during the technical evaluation: A penalty amount of Rs. 50,000/- would be applicable to the successful bidder per substitution per CV / resume proposed with the technical bid.	The clause stands deleted. The bidders need to abide by clause 3.10.2 Technical evaluation Sr. no. 6 & 7 as per the corrigendum
86.	11.1.3 Manpower	106	Substitution of Resources from those whose CVs provided during the technical evaluation	The clause stands deleted. The bidders need to abide by clause 3.10.2 Technical evaluation Sr. no. 6 & 7 as per the corrigendum

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
87.	11.1.3 Manpower	106	Penalty for Replacement of resources during operations and maintenance phase: A penalty of 0.1% of the total cost of project would be applicable to the successful bidder for every replacement deviating from the SLA	The modified clause to be read as: "A penalty of 1% of the QGR value for the quarter period the resource leaves until the quarter period the replacement resource joins would be applicable to the successful bidder for every replacement deviating from the SLA."
88.	11.1.3 Manpower	106	SLA 2. No substitution of resources would be allowed whose CVs/ resumes had been provided with the technical bid against RFP within 180 days from the submission of the bid (except in case of death, medical incapacity or resignation).	The modified clause to be read as: "Substitution of resources would be allowed whose CVs / resumes had been provided with the technical bid against the RFP within 180 days from the submission of the bid (except in case of death, medical incapacity or resignation), also provided that the actual resources deployed are at par with the CVs and interviewed personnel, otherwise the bidder has to deploy the resources whose CVs and interview was shared with OCAC. A penalty amount of Rs. 50,000/- would be applicable to the successful bidder per CV / resume proposed with the technical bid if found non-compliant."
89.	Proforma 16: Financial Proposal – IT and Non-IT (CAPEX)/Network and 13.2 Non-IT assets	164 & 111	LED Display (70 inch)	The modified clause to be read as: "Videowall cube 70" in (4x2 matrix)"
90.	14.1 General terms	112	1. All solutions proposed by the bidder should be of latest manufacturing product and not more than 01 year old from the bid submission date, latest configuration and should not reach end of life or end of support for at least 07 years after installation.	The modified clause to be read as: 1. All solutions proposed by the bidder should be of latest manufacturing product and not more than 01year old from the bid submission date, latest configuration and should not reach end of life or end of support for at least 05 years after installation.

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
91.	14.6 Liquidated damages	115	If the implementation agency fails to deliver any or all of the services within the time period(s) specified in the RFP, OCAC shall without prejudice to its other remedies under agreement, deduct from the Agreement Price, as liquidated damages, a sum equivalent to, as per the SLA terms indicated in the bid document, until actual delivery or performance, subject to a maximum of 20% of the project value / project cost quoted by the bidder.	The modified clause to be read as: "subject to a maximum of 10% of the project value / project cost quoted by the bidder." Rest of the clause to remain the same.
92.	14.6 14.6 Liquidated damages	115	Liquidated damages If the implementation agency fails to deliver any or all of the services within the time period(s) specified in the RFP, OCAC shall without prejudice to its other remedies under agreement, deduct from the Agreement Price, as liquidated damages, a sum equivalent to, as per the SLA terms indicated in the bid document, until actual delivery or performance, subject to a maximum of 20% of the project value / project cost quoted by the bidder.	The modified clause to be read as: "subject to a maximum of 10% of the project value / project cost quoted by the bidder." Rest of the clause to remain the same.
93.	16. Exit Management 16.1 Purpose	123	The exit management period starts, in case of expiry of agreement, on the date when the agreement comes to an end or in case of termination of agreement, on the date when the notice of termination is sent to the successful bidder.	The modified clause to be read as: "- The exit management period starts, 03 months prior to expiry of agreement as on the date when the agreement comes to an end or in case of termination of agreement, on the date when the notice of termination is sent to the successful bidder.

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
94.	Proforma 6: Format of Earnest Money Deposit (EMD)	144	In consideration to the advertisement published by OCAC (hereinafter called the "Purchaser") has their offer dated_____ through RFP for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre at OCAC, Bhubaneswar hereinafter called the "IA") against the purchaser's RFP enquiry No. ____/_____/_____ KNOW ALL MEN by these presents that We _____< Bank Name> of _____ having our registered office at _____ are bound unto _____ (hereinafter called the "Purchaser) in the sum of _____ for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents.	Revised Proforma 6: Format of Earnest Money Deposit (EMD) as per the Letter no. 27928/F FIN-COD-MISC-0008-2017 dated 16-10-2020 from Finance Department. Revised format provided below.
95.	Proforma 8: Undertaking of Service Level	148	2. However, if the proposed resources, Non-IT Infrastructure and ICT components are found to be insufficient in meeting the RFP and/or the service level requirements given by OCAC, then we will augment the same without any additional cost to OCAC	The modified clause to be read as: However, if the proposed resources, Non-IT Infrastructure and ICT components are found to be insufficient in meeting the RFP and/or the service level requirements given by OCAC, then we will augment the same without any additional cost to OCAC; provided such insufficiency is solely attributable by the Implementing Agency
96.	Proforma 9: Warranty Certificate	149	----------------------------	Revised Proforma is given below in the document.

Sr. No.	RFP Clause No.	RFP Page no.	Existing Clause Details	Modification / Remarks
97.	Proforma 11: Proposal Covering Letter – Technical	152	We are hereby submitting our Proposal, which includes this Technical bid as per the Proforma, eligibility criteria and other relevant terms and conditions of the RFP. We hereby declare that all the information and statements made in this Technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification. We agree to abide by all the terms and conditions of the RFP document. We would hold the terms of our bid valid for 180 days as stipulated in the RFP document.	The modified clause to be read as: We are hereby submitting our Proposal, which includes this Technical bid as per the Proforma, eligibility criteria and other relevant terms and conditions of the RFP. We hereby declare that all the information and statements made in this Technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification. Subject to the deviations submitted along with the proposal; 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.
98.	Proforma 13: Project Credentials Format	154	Project Details: 9. Effort involved in Payroll person-months in the complete project	This point stands deleted.
99.	Proforma 14: Format for providing CV of Manpower to be proposed	156	Table B 17. Signature of the representative	The modified clause to be read as: 17. Signature of the representative / authorized signatory
100.	Proforma 22: Format of Bank guarantee	170	Proforma 22: Format of Bank guarantee	Revised Proforma 22: Format of Bank guarantee as per the Letter no. 27928/F FIN-COD-MISC-0008-2017 dated 16-10-2020 from Finance Department. Revised format provided below.

The following clauses / scope are in addition and to be read as a part of RFP Enquiry number: OCAC-TE-17/2018(P-I)/ENQ-20030, Date 24.09.2020.

Addition of deviation clause and Proforma:

Clause 17: Deviations and Exclusions

Bidders shall submit bid strictly in accordance with the requirements and terms & conditions of the RFP. The bidder shall submit a Statement of No Deviation document as per the format specified in Proforma 25 (provided below in the document). The bids without the deviation certificate are liable for rejection.

Addition to Section 4: Scope of work

Bug Bounty

A bug bounty program is an opportunity offered by many websites, organizations and software developers by which individuals can receive recognition and compensationfor reporting bugs, especially those pertaining to security exploits and vulnerabilities.

Scope of activity:

1. Crowd sourced hunting of bugs and vulnerabilities of Odisha State citizen centric websites / applications.
2. The scope is limited to the websites / applications that are hosted in Odisha State Data Centre (OSDC), Odisha Sate Wide Area Network (OSWAN) and State IT Centre.
3. Bidder to validate the vulnerabilities found for false positive and report only the validated and authentic vulnerabilities to OCAC.
4. The hosted website / applications may be owned by various departments and the bidder needs to coordinate with the respective department for the activity.
5. Bidder needs to trace any bug / vulnerability and report to OCAC with recommendation.
6. Supply, installation and commissioning of all infrastructure required for the activity.
7. Integration with existing infrastructure for implementation of Bug bounty activity.
8. Creation of test environment and creation of pseudo data / information for the activity.
9. Handholding support with respective departments for the implementation, completion and closure of the activity.
10. Award of appreciation / bounty to the participant who contributed in finding critical vulnerabilities.

Addition to Section 7 Minimum technical requirement (IT assets):

Section 7.15 Bug Bounty program

Sr. No.	Requirement Description
1.	The platform should be based out and operated within India.
2.	The Crowdsourced Bug Bounty platform should have relevant experience and should be recognized by leading analysts such as Gartner / Forrester, etc.
3.	The platform should have the ability to support both Public (Open to all) as well as Private (By invite only) bug bounty program.
4.	The platform should maintain a record of all security researchers with their valid Identity proof, legal contracts, communication address, and user activity.
5.	The platform should allow triaging of vulnerabilities and label them as valid, invalid, informative or duplicate.
6.	The platform should be capable of configuring and assigning roles to researchers and OCAC and also able to segregate role-based access control.
7.	The platform should support discovery of all OWASP top10 & recent attack vectors.
8.	The platform should support private deployment and the applicationtogether with all related data should be hosted on-premise or on specific infrastructure provided.
9.	The handling of vulnerabilities should follow ISO/IEC 29147:2014 or similarsecurity standards and the workflow should ensure that vulnerability reports cannot be accessed by anyone other than those authorized.

Addition to Section 14.1 General terms:

1. It is under the discretion of the respective department / OCAC to authorize for the Bug bounty activity.
2. All data related to the Bug bounty activity would be on-premises, no data would be authorized to be taken outside OCAC premises.
3. The bidder to assess the requirement and propose the required hardware / solution for the Bug bounty activity.
4. 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.
5. The Bug bounty activity should not utilize production assets and the successful bidder is to create the staging or testing environment for the establishment of identical environment.
6. All the information (public / private) on the existing asset is not to be utilized for the Bug bounty activity and bidder should create pseudo data for the activity.
7. Under the authorization of OCAC, the bidder to coordinate with the respective department for the Bug bounty activity and environment establishment.
8. The proposed financial cost of the Bug bounty activity would include all aspects and no additional cost for the hardware / solution would be borne by OCAC.
9. In no case the result of Bug Bounty should be made public. The bidder should be compliant to Non-Disclosure Agreement (NDA) mutually signed between OCAC and bidder in this regard.
10. Any award or bounty towards the participant would be the responsibility of the bidder after successful completion of the Bug bounty activity.

Addition to Section 12: Reporting

Sr. No	Deliverable Name	Deliverable timeline / frequency	Report to be shared with
11	Bug Bounty activity	As and when requested by OCAC. a. Vulnerability findings during the activity. b. Validation report of the vulnerabilities. c. Recommendations as per the vulnerability findings. The frequency of activity may be increased after evaluation of the performance of the bidder in terms to the activity.	Department SPOC / GM (Admin) / Joint GM (Tech) / PMU

Addition to Section 11: Payment terms

Sr. No.	Activity	Payment terms	Remarks
1	Bug Bounty	100% payment on completion of activity.	Submission of: 1. Proof of concept for the vulnerability findings. 2. Recommendation for the closure of the vulnerability.

Proforma 25: Statement of No Deviation from minimum technical requirement

RFP Ref. No.: OCAC/_____/____   Date:

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

Sir,

There are no technical deviations (null deviations) from the minimum technical requirement of tendered items and schedule of requirements. The entire work shall be performed as per your specifications and documents.
This is to certify that our proposed solution meets all the requirements of the RFP including but not limited to Scope of Work, stated Project Outcomes (including SLAs), Business Requirements and Functional Specifications/ Requirements.

We further certify that our proposed solution meets, is equivalent or better than the minimum technical requirement as given in the RFP.

We understand that the Bill of Materials provided in the RFP is indicative, we confirm that we have undertaken our own assessment to finalize the components and quantity.

In case, any item of hardware or software is found non-compliant at any stage during project implementation, it would be replaced with a fully compliant product/solution at no additional cost to OCAC. In case of non-adherence of this activity, OCAC reserves the right to cancel the contract, in case the said Contract is awarded to us by OCAC.

We further confirm that our commercial proposal is for the entire scope of work, comprising all required components and our obligations, for meeting the scope of work.

Thanking you,

Yours sincerely,

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

Name: Place:
Designation: Date:

Revised Proforma 6: Format of Earnest Money Deposit (EMD)

Whereas……………………………………………………. (hereinafter called the "tenderer") has submitted their offer dated_____ for the supply of …………………………………………….(hereinafter called the "tender")against the purchaser's tender enquiry No. _____

KNOW ALL MEN by these presents that We _____ of _____ having our registered office at _____ are bound unto _____ (hereinafter called the "Purchaser) in the sum of _____ for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents.

Sealed with the

Common Seal of the said Bank this _____ day of _____, 2020.

THE CONDITIONS OF THIS OBLIGATION ARE:

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

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

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

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

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

This guarantee will remain in force up to and including 45 days after the period of the tender validity and any demand in respect thereof should reach the Bank not later than the above date.

Our…………………………………………branch at………………………………..*(Name and Address of the ……………* branch) is liable to pay the guaranteed amount depending on the filing of claim and any part thereof under this Bank Guarantee only and only if you serve upon us at our …………………………* branch a written claim or demand and received by us at our ………………….* branch on or before Dt………………………………otherwise bank shall be discharged of all liabilities under this guarantee thereafter.

_____

(Signature of the authorized officer of the Bank)

_____

Name and designation of the officer

_____

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

Preferably at the headquarters of the authority competent to sanction the expenditure for purchase of goods or at the concerned district headquarters or the State headquarters.

Revised Proforma 22: Format of Bank guarantee

To,

    The Governor of Odisha

WHEREAS………………………………………………………. (name and address of the supplier) (hereinafter called the "supplier") has undertaken in pursuance of contract no…………………………………….. dated_____ to supply of ………………………………………………..(description of goods and services) (hereinafter called the "contract").

AND WHEREAS it has been stipulated by you in the said contract that the supplier shall furnish you with a bank guarantee by a scheduled commercial bank recognized by you for the sum specified therein as security for compliance with its obligations in accordance with the contract:

AND WHEREAS we 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 ………………………………………………..(amount of the guarantee in words and figures), 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 limit of (amount of guarantee) as aforesaid, without you 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 supplier 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 thereunder or of any of the contract documents which may be made between you and the supplier 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 the…………………day of ………………, 20………

Our……………………………………..branch at…………………………………..*(Name and Address of the ……………* branch) is liable to pay the guaranteed amount depending on the filing of claim and any part thereof under this Bank Guarantee only and only if you serve upon us at our ……………………………* branch a written claim or demand and received by us at our ……………………..* branch on or before Dt………………………………otherwise bank shall be discharged of all liabilities under this guarantee thereafter.

_____

(Signature of the authorized officer of the Bank)

_____

Name and designation of the officer

_____

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

Preferably at the headquarters of the authority competent to sanction the expenditure for purchase of goods or at the concerned district headquarters or the State headquarters.

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

(To be declared in bidder's letter head)

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

Sr. No	Item Description	UoM	QTY$	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E = D%*C	F = C+E
Desktop / Printer										
1	Desktop	Nos.	17							
2	LED monitors - additional	Nos.	16							
3	Multifunction printer	Nos.	1							
Non – IT assets (Indicative)										
Civil and Interiors										
1	Flooring									
a	False flooring	Sqr Mtr	Bidder to Propose							
b	Italian Marble / Composite stone flooring	Sqr Mtr	Bidder to Propose							
c	Carpet flooring	Sqr Mtr	Bidder to Propose							
2	Partitions and Paneling	Sqr Mtr	Bidder to Propose							
3	Paint	Sqr Mtr	Bidder to Propose							
4	Doors									
a	Double leaf glass door	Nos.	Bidder to Propose							
b	Fire rated steel door	Nos.	Bidder to Propose							
c	Fire rated toughened glass door	Nos.	Bidder to Propose							
5	False ceiling	Sqr Mtr	Bidder to Propose							
a	Metal Baffle ceiling	Sqr Mtr	Bidder to Propose							
b	Designer Acoustic false ceiling	Sqr Mtr	Bidder to Propose							

Sr. No	Item Description	UoM	QTY$	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E =D%*C	F = C+E
c	Curvilinear or designer ceiling	Sqr Mtr	Bidder to Propose							
6	Air Conditioning	Sqr Mtr	Bidder to Propose							
7	Electrical Wires, Switches & Conduits for ceiling and floor lights	Sqr Mtr	Bidder to Propose							
8	Passive Cabling with components	Sqr Mtr	Bidder to Propose							
9	LED Ceiling lights									
a	General LED lights	Nos.	Bidder to Propose							
b	Circular / Dimmable LED lights	Nos.	Bidder to Propose							
c	LED strips	Nos.	Bidder to Propose							
10	Distribution Board with Electrical MCB complete	Nos.	Bidder to Propose							
11	Modular switch board with switches and sockets for Desk with complete wiring	Nos.	Bidder to Propose							
12	Earth pit	Nos.	3							
13	Perforated cable tray (factory made galvanized)	Mtr	Bidder to Propose							
14	Cable raceway for cabling and wiring	Mtr	Bidder to Propose							
Electrical										
1	UPS - 20 KVA	Nos	2							
2	Battery bank	Set	2							
Furniture										
1	Command centre control desk - 8 seater capacity	Nos.	2							

Sr. No	Item Description	UoM	QTY$	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E =D%*C	F = C+E
2	Manager Table	Nos.	1							
3	Meeting room table	Nos.	1							
4	Reception Table	Nos.	1							
5	Command centre chair	Nos.	16							
6	Chair for office and reception	Nos.	6							
7	Manager's chair	Nos.	1							
8	Storage Units	Nos.	2							
9	Staff Locker unit	Nos.	Bidder to Propose							
10	Key Box	Nos.	1							
11	Dust bin (Stainless steel)	Nos.	4							
12	White board - Glass pasted	Nos.	2							
13	Sofa set	Nos.	2							
14	Coffee table	Nos.	1							
15	Pin up Notice board	Nos.	2							
Safety & Security System										
1	Close circuit tele vision (CCTV) NVR - 16 channel	Nos.	1							
2	Dome camera – IP based	Nos.	9							
3	32-inch Display screen	Nos.	2							
4	Door Access control system for 8 access controls with main panel & software	Set	1							
5	Rodent repellant system	Set	1							
6	Fire extinguisher - handheld	Nos.	5							
7	Addressable Fire Detection and Alarm system with software (20 detectors, 3 sirens)	Set	1							
Network										
1	42U Rack with 48 port jack panel	Nos.	1							
2	Videowall cube 70" in (4x2 matrix)	Nos.	8							

Sr. No	Item Description	UoM	QTY$	OEM / Make	Model / Part Detail	Unit Price (in Rs.)	Total price excluding tax (in Rs.)	Tax rate (%)	Tax amount (in Rs.)	Total Price including tax (in Rs.)
			A			B	C = A*B	D	E =D%*C	F = C+E
3	Video wall controller & speakers with all accessories	Set	1							
Installation and Commissioning										
1	One-time implementation cost	Lot	1							
	Total amount (sum of all values in column C, E and F)									
	Total CAPEX cost (sum of all values in column F)									
	Total CAPEX cost in words (sum of all values in column F)									

Note:

* Log Management appliances should be proposed as 4 nos. in quantity if existing asset is to be upgraded and utilized and 6 nos. quantity to be proposed if new assets and solutions are to be proposed by the bidder. The log management appliances / solution shall be placed in pairs in OSDC, OSWAN and State IT centre. Each solution should be as per the minimum technical requirement mentioned in the RFP.

SIEM QTY should be proposed as 0 nos. (zero) and cost should be mentioned if existing asset is to be upgraded and utilized. SIEM QTY should be proposed as 1 no. (One) and cost should be mentioned if new asset and solution is to be proposed by the bidder.

^Bug Bounty to be considered as an activity. The bidder to assess and propose cost which would include all aspects of the activity regarding infrastructure, software, timeline and scope of work. The cost proposed would be for only one application / website and OCAC may increase the number of application / websites based on the performance of the bidder at any period of the project. The cost proposed is to be fixed for the contract period.

$The column in financial proposal where the quantityis for the bidder to propose, the minimum of proposed quantity by all bidders will be used for computation of the bid price.

Revised Proforma 20: Financial Proposal – Additional cost

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

Additional Manpower (temporary if required on request from OCAC)

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

Additional licensing / tools

Sl. No	Manpower description	Quantity / Capacity	Make & Model	Unit price (in Rs.)	Total Price (in Rs.)	Tax rate (%)	Total tax amount (in Rs.)	Total price including tax (in Rs.)
		A		B	C=A*B	D	E=D%*C	F=C+E
1	Vulnerability management solution license – per device / per IP							
2	User licenses (to be added by bidder) – per device / per user							
3	Storage per 01 TB in SAN							
4	Creation of 01 playbook in SOAR							
5	Cost of additional 1000 EPS							
6	*Any other solution to be proposed by the bidder can be mentioned by adding rows to the table**							
				TOTAL				
				TOTAL (in words)				

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

Revised proforma 9: Warranty Certificate

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

Date:……………..

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

Sir/Madam,

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

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

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

Yours sincerely,

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

Name: Place:
Designation: Date:

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

(To be declared in the bidder letter head)

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

Subject: Self-declaration for clean track record of services

Sir,

To the best of our knowledge and as per records available with the company,I hereby declare that my company…………………………. has not been debarred / blacklisted by Government of India / Government of Odisha in the last three years for indulging in corrupt or fraudulent practices or for indulging in unfair trade practices and not backed out from executing the work after award of the work as on the RFP submission date.

As per records available with the company, my company…………………………… is also not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this RFP.

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

Yours sincerely,

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

Name: Place:

Designation: Date:

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
1	3.1 Bid Schedule Earnest Money Deposit - (EMD)	13	Rs. 50,00,000/- (Fifty lakhs only) in form of Bank Guarantee in the prescribed format in favour of "OCAC" payable at Bhubaneswar from a nationalized / scheduled commercial bank in India.	1. Kindly provide EMD validity and Bank details for SFMS confirmation. 2. Can the EMD be reduced ?	EMD need to be valid upto 6 months from the date of submission of bid. Proforma 6 provided for the EMDCorrigendum
2	3.5 General Instructions to bidders	15	The bidder shall be responsible for the upgradation and additional configuration of the SIEM (ArcSight ESM) solution, Logger appliances, Connector appliances and User Behavioural Analyser (UBA) appliance which are installed at Odisha State Data Centre.	1. We understand that Existing SIEM has enough Storage and Compute for future Upgardation.Plese confirm. 2. The existing Arcsight SIEM has integrated UBA solution. If bidder wants to propose a new SIEM with Logger/Connector solution then do they need to consider UBA as well? In that case pls share if there is any specific use cases on UBA or any technical specifications are available. 3. The RFP states that bidder can propose new SIEM solution in case bidder does not intend to re-use the eisting SIEM, logger and connector solutions. However, UBA solution is also present. Kindly clarify whether bidder is required to re-use existing UBA solution or free to proposed new UBA solution.	1. The bidder in case proposes a new SIEM solution, then the existing solutions needs to be integrated with the new proposed SOC. 2. Any further details regarding the existing solutions would be provided to the successful bidder. 3. A new UBA solution is not to be proposed by the bidder. The existing UBA solution shall be integrated to the proposed SOC.
3	3.8 Submission of bid	17	Virtual walkthrough of existing Cyber SOC command centres implemented by the bidder.	1. This may need some kind of permissiom from existing customers. Kindly confirm Can we do a virtual walkthrough of our shared SOC?	Virtual walkthrough of any on-premises SOC established by the bidder would be preffered. Incase there is any limitation or challenge, the bidder may present a virtual walkthough of their shared SOC premises.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
4	3.10.1 Eligibility criteria, SI No-1	20	A bidder with solutions developed in an entity incorporated in a country sharing a land boundary with India cannot participate in this bid.	1. Make in India is an initiative by the Government of India to encourage companies to manufacture in India and incentivize dedicated investments into manufacturing. As per this guideline purchase preperence shall be given to local suppliers. Therefore we are request your good office to modify the clause as "A bidder with solutions developed in an entity incorporated in a country sharing a land boundary with India cannot participate in this bid. Make in India solution having Global Presence will get added advantahges." 2. This requirement is not clear. Most of the OEM's may have/had R&D or support activities (directly or indirectly) in countries that share land-border with India. Are they permitted to bid? The reason is very simple since according to the data-sharing norms under a their law, companies are	The bidder should propose solution from entity which have all solution related processes / developments from countries not sharing a land boundary with India.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
5	3.10 Criteria for bidding eligibility and evaluation 3.10.1 Eligibility criteria	20	The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.12.2019. SOC solution could be On-premises SOC, Managed SOC, Hybrid SOC. At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5 crore.	1. We understand this clause as follows:- The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.12.2019. SOC solution could be On-premises SOC/ Managed SOC/Hybrid SOC. At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services. Minimum value of any one project should be above 5 crore. In most of the Projects, SOC Room shall be part of either Command Control Centre or Data Centre. Hence Request you to accept project with either SOC solution or Project with SIEM Supply,Installation,commissioning and O&M scope. Please confirm Projects in which O&M yet to start or O&M under progress is also accepted against this eligibility criteria.	Modification: 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 5 crore.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
6	3.10.1 Eligibility criteria; Sr No: 5	20	The bidder should have a minimum average annual turnover of at least Rs. 200 Crores in the last three financial years (i.e. 2016-17, 2017-18 & 2018-19).	1. The bidder should have a minimum cumulative turnover of at least Rs. 275 Crores in the last three financial years (i.e. 2016-17, 2017-18& 2018-19). 2. Kindly amend the below clause as: 5. The bidder should have a minimum average annual turnover of at least Rs. 200 Crores in the last three financial years (i.e. 2016-17, 2017-18, 2018-19, 2019-20)	Modification: " The bidder should have a minimum average annual turnover of at least Rs. 200 Crores in the last three financial years (i.e. 2017-18, 2018-19 & 2019-20). In case the bidder does not have the audit financial statements then a letter under the head of the chartered accountant / or firm certifying the financial turnover of the company is to be submitted with the bid. In case the bidder faces challenge in the letter submission, then bidder may submit the audited financial statements for financial years (i.e. 2016-17, 2017-18 & 2018-19). " As per MeitY guidelines the average annual turnover is fixed.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
7	3.10 Criteria for bidding eligibility and evaluation 3.10.1 Eligibility criteria, serial no 10.	20	The bidder should have minimum manpower strength as per the different skill levels defined in the document: Level 1 analyst – minimum 20. Level 2 analyst – minimum 20. SME level - minimum 3. (The manpower criteria as mentioned in the Section 8.2 and 8.3 of the RFP document) All manpower should be on the pay role of the company / bidder.	1. We request you to modify this clause :- The bidder should have minimum manpower strength as per the different skill levels defined in the document: Level 1 analyst – minimum 5. Level 2 analyst – minimum 2. SME level - minimum 1. (The manpower criteria as mentioned in the Section 8.2 and 8.3 of the RFP document) ~~All manpower should be on the pay role of the company / bidder.~~ We request you to modify this clause :- The bidder should have minimum manpower strength at time of Manpower Deployment as per the different skill levels defined in the document: Level 1 analyst – minimum 20. Level 2 analyst – minimum 20. SME level - minimum 3. (The manpower criteria as mentioned in the Section 8.2 and 8.3 of the RFP	All manpower mentioned should be working under the bidder and working in any SOC project.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
8	3.10 Criteria for bidding eligibility and evaluation 3.10.1 Eligibility criteria, serial no11	21	The bidder should be: □ ISO 9001:2008 or later certified □ ISO 20000: 2018 certified □ ISO 27001: 2013 certified	1. We request the buyer to kindly clarify if a certificate under process shall be acceptable for satisfying the criteria for Bidder/OEM. 2. We request you to kindly modify as follows : The bidder should be any two of following : □ ISO 9001:2008 or later certified □ ISO 20000: 2011 certified or latest □ ISO 27001: 2013 certified However Bidder shall be responsible for delivering end to end this project and abide all the ISO Standards. We understand that Bidder can submit their Subsidiary Company ISO Credential as well. Please confirm The bidder should be : □ ISO 9001:2008 or later certified □ ISO 20000: 2011 certified or latest □ ISO 27001: 2013 certified However Bidder shall be responsible for delivering end to end this project and abide all the ISO Standards	Modification: The bidder should be: □ ISO 9001:2008 or later certified □ ISO 20000: 2011 or later certified □ ISO 27001: 2013 or later certified

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
9	3.10.1 Eligibility criteria	21	6. The bidder should have positive net worth during the last three financial years (i.e. 2016-17, 2017-18 & 2018-19).	1. Request Dept. to kindly revise the clause as below : " The bidder/bidder's parent company should have positive net worth during the last three financial years (i.e. 2016-17, 2017-18 & 2018-19)." 2. Request to change "Audited Balance Sheets for last 3 years, i.e., 2016-17, 2017-18 & 2018-19 where profit or loss . Every sheet should be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 3 financial years." - As Profit and loss for each project not mentioned in Balance sheet 3. Kindly amend the below clause as: 6. The bidder should have positive net worth during the last three financial years (i.e. 2016-17, 2017-18, 2018- 19, 2019 - 20) 1) The CA certificate has to clarify the profit & loss of the company from similar line of services. What is	No change proposed.
10	3.10.1 Eligibility criteria	21	The bidder should have local office in Odisha or should submit a declaration for establishing an office in Odisha within one month of issuing of Letter of Intent (LoI) from OCAC.	1. Is this a mandatory requirement ? 2. We request OCAC to allow atleast 3 months from contract signing date to open a project office by the bidder. 3. Preference should be given for local presence of company and mark should be distributed	The timeline provided is sufficient for the criteria.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
11	3.10 Criteria for bidding eligibility and evaluation 3.10.2 Technical evaluation	22	Experience in implementation of on-premises Cyber Security operations centre.	1. In most of the Project, Cyber Security operations centre shall be part of either Command Control Centre or Data Centre. Hence Request you to accept project with SIEM Supply,Installation,commissioning and O&M scope. 2. 2. Experience in implementation / management of on premises Cyber Security Solution 3. Request Dept. to Kindly revise the clause as below : "Experience in implementation of onpremises Cyber Security operations centre/Managed NOC.	The bidder should have an experience of On-premises SOC implementation as it the basic requirement of our project. Odisha SOC is a On-premises project and any bidder without previous expereince would only value add to the project.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
12	3.10.2 Technical evaluation	23	Point No 3. The proposed bidder / OEM has experience in implementing at least one project handling 20000 EPS or more	1. Request Dept. to kindly revise the clause as below : " The proposed bidder / OEM has experience in implementing at least one project handling 20000 EPS/150 devices or more. 2.The proposed bidder / OEM has experience in implementing at least one project handling 20000 EPS or more Document to be Submitted: Relevant MSA copy / Work order copy / client satisfactory letter mentioning the number of EPS and the solution. The WO / letter should be in the name of the bidder / OEM ~~and clearly mention the scope~~ of work. Marks distribution: More than 10000 EPS = 10 marks More than 5000 EPS up to 10000 EPS = 7 Marks 2000 EPS up to 5000 EPS = 5 Marks 3. We are giving a device based	The criteria is considered keeping the minimum techincal requirement and criticality of the project.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
13	3.10.2 Technical evaluation SI No-4	23	Major solutions like SOAR and SIEM should be from OEMs who have both local and global presence, deployed solutions and supported customers globally. Yes, have both national and global presence = 05Mark No, does not have both national and global presence = 00Mark	As per RFP Clause 3.5 General Instructions to bidders, the bidder may propose "Make in India" products and solutions in their bid. So we are requesting your good office, please provide preferance to "Make-in India" OEM/Solution as per Govt. Of India guideline and request to modify the Clause " Major solutions like SOAR and SIEM should be from OEMs who have both local and global presence, Make in India solutions and supported customers globally." 2. Marks should be given to Make in India solution as well in keeping with the Atmanirbhar Initiative of Govt of India along with global presence	The evaluation criteria is kept as per the criticality of the solution and requirement.
14	3.10 Criteria for bidding eligibility and evaluation 3.10.2 Technical evaluation, serial no 6	23	Quality of the CVs of resources proposed for the CSOC project SOC Manager Security administration and Threat Intelligence expert CSOC Engineer - 0.5 marks for each resource Level 2 Analyst - 0.5 marks for each resource Level 1 Analyst - 0.5 marks for each resource	We understand that Bidder need to propose following Nos of Manpower to obtain full Marks:- SOC Manager- 1 No. Security administration and Threat Intelligence expert- 1 No. CSOC Engineer -3 Nos. Level 2 Analyst - 7 Nos. Level 1 Analyst -7 Nos. Total - 19 Numbers	The evaluation criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
15	3.10 Criteria for bidding eligibility and evaluation 3.10.2 Technical evaluation, serial no 7	23	Quality of resources to be proposed for CSOC operations SOC Manager Security administration and Threat Intelligence expert CSOC Engineer - 1.5 marks for each resource Level 2 Analyst - 1 marks for each resource Level 1 Analyst - 1 marks for each resource	We understand that Bidder need to propose following Nos of Manpower to obtain full Marks:- SOC Manager- 1 No. Security administration and Threat Intelligence expert- 1 No. CSOC Engineer -3 Nos. Level 2 Analyst - 7 Nos. Level 1 Analyst -7 Nos. Total - 19 Numbers	The evaluation criteria is kept as per the criticality of the solution and requirement.
16	3.10 Criteria for bidding eligibility and evaluation 3.10.2 Technical evaluation	23	6. Quality of the CVs of resources proposed for the CSOC project 7. Quality of resources to be proposed for CSOC operations	We request you to kindly decrease the Manpower CV as follows:- SOC Manager- 1 No. Security administration and Threat Intelligence expert- 1 No. CSOC Engineer ~~3~~ 1 Nos. Level 2 Analyst - ~~7~~ 2 Nos. Level 1 Analyst ~~7~~ 4 Nos. However Bidder undertakes that Manpower shall be deployed post award of contract as per Customer expectations. We understand that Bidder proposed manpower need not be on Bidder's Payroll, as manpower taken from local enterprise is also acceptable as per clause 3.5, General Instruction to bidders, page 16. Please confirm	The evaluation criteria is kept as per the criticality of the solution and requirement.
17	3.10.2 Technical evaluation,sl.no. 8 and 9	24	Technical presentation to be given by the bidder to OCAC. Marks would be awarded as per the technical committee of evaluation from OCAC.	Since, there is no marks allocated to the technical proposal of bidder, we request OCAC to allocate 10 marks for the technical proposal and 10 marks for the technical presentation.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
18	3.10.3	26	Financial evaluation The Evaluation Methodology proposed to be adopted by OCAC will be Quality cum Cost Based System (QCBS) method of evaluation where Technical Bid Score will get a weightage of 70% (denoted by ST) and Commercial Bid Score a weightage of 30% (denoted by SF).	The bidder requests the following modifications: The Evaluation Methodology proposed to be adopted by OCAC will be Quality cum Cost Based System (QCBS) method of evaluation where Technical Bid Score will get a weightage of 80% (denoted by ST) and Commercial Bid Score a weightage of 20% (denoted by SF).	The criteria is kept as per the criticality of the solution and requirement.
19	4	27	Security Product Management	1. Please clarify for what all devices, security product management is in scope? As per our understanding, the infrastucture at Odisha State Data centre, SWAN and State IT centre is not in scope. Only its security event monitoring is in scope. Please detail the infrastructure for which Security Product Management is in scope? 2. We request OCAC to kindly provide the count (approximate) of security products that are to be procured by OCAC in future. another query under same subheading: We understand that If the tool requires any specialised skill, deployment of manpower will be done on mutual agreement basis for technical implementation and monitoring. Please confirm.	Security Product Management is limited to SOC infrastructure only.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
20	4. Scope of work for bidder Security Product Management:	27	The services will include : a. Configuration, fault, performance and availability management of the CSOC infrastructure. b. Activities like but not limited to; patch management, firmware upgrade, configuration backup.	1. Are licence for projects individual project based and OCAC has to oversee or perform these activities. Kindly clarify 2. We understand that security product management activities will be carried out for security components propsoed as part of this RFP. Kindly confirm.	Security Product Management is limited to SOC infrastructure only.
21	4. Scope of work for bidder	27	Service provider resources are expected to deliver SOC services including but not limited to performance monitoring, performance tuning, optimization, and maintenance of CSOC security tools, SIEM log backup, troubleshooting, security monitoring, security product management, vulnerability assessment and penetration testing and application security testing.	1. The requirement of Penetration testing and application security testing is not clear. Please share the specifications for both the requirements. The number of external IPs for PT and number of applications for Application security testing. 2. Please share the existing Vulnerability Management solution deployed in OCAC's environment? Can bidder leverage same? As per the bidder, security product management comprises of managing the devices deployed in CSOC center? Is this understanding correct? Or there are any other security tool eg firewall, EDR, Antimalware, Proxy, dlp which OCAC is expecting bidder to manage? Bidder understands that VA is only to be done for the devices and tools deployed in CSOC center? Is this understanding correct?	1.Application testing would be under the scope of Vulnerability Management system for vulnerability scanning / assessment only. The application vulnerability assessment / testing would be on need basis only under the scope of Vunerability Management solution. 2. The proposed Vulnerability Management solution would be independent of any existing solution. 3. Security Product Management is limited to SOC infrastructure only.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
22	4. Scope of Work, Paragraph-3	27	Initially implementation of CSOC is to be carried out for the above three stakeholders. On reaching stability and maturity of CSOC system, additional stakeholders would be added to the project and the scope of work for the bidder would be expanded covering the additional stakeholders also. The bidder should propose cost for the project as per the format / proforma provided in the RFP document.	We request to clarify of the number departments planned to be integrated in the future, requirements on the future enhancements and percentage of enhancements to analyse tool dependencies may kindly be done at OCAC end including commercial impact to operating agency	The number of department is not finalized. Sizing and scalability is taken into account for addition of departments. Any further scalability, other than the proposed capacity would be done with mutual agrrement of OCAC and successful bidder.
23	4. Scope of Work, 2nd sub heading	27	Security Monitoring Service This service will help OCAC to monitor for security events throughout its network by analysis of logs from servers, devices and key applications.	We request to clarify that what is the level of involvement of application developer in integrating the application log sources?	Bidder to assess about the integration and technology and propose.
24	4. Scope of Work, 2nd sub heading, bullet no 6	27	Extend Security to all Critical Infrastructure of the State (e.g., SDC, SWAN, IT Centre, etc.).	We request to clarify the requirement here on extended security - any specific tools are expected to be implemented over a period of time / provide security roadmap. As per our understanding, bidder must provide security monitoring services to projects including Odisha State Data Centre (OSDC), State-wide Area Network (SWAN) and State IT Centre. As the clause contains the word "etc", we request OCAC to kindly mention clearly on the projects to be integrated with CSOC without any ambiguity.	Bidder to assess and propose solutions as per the BOM proposed in the RFP.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
25	4. Scope of work for bidder	28	Vulnerability Management Services: Conduct VAPT and Application Security tests as in when required	1. Kindly confirm the application security to consider as services or dedicated application security solution needs to be factoerd ,if it is dedicated app security Provide the technical specification for the same and request to add it in BOQ Kindly Provide the frequency of time span to conduct the application security testing. 2. We request to clarify on tools / utilities expected here. As per our understanding bidder may use commercial/open source tools in order to perform vulnerability assessment and penetration testing. Please confirm. another query under same subheading: We request to clarify on the Department wise BOM for which hardening rules to be developed. We understand implementation will be done by the department IT service provider. Please confirm.	Application testing would be under the scope of Vulnerability Management system for vulnerability assessment nad Bug Bounty. The testing would be done on need basis.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
26	4. Scope of work for bidder	28	c. Bidder has to provide tools / utilities and skilled resources to conduct the respective tests.	In RFP, specificaion of Vulnerability Assessment tool is present but Penetration testing and Applications Security testing specifications are not available and the requirement is also not clear. Please share the requirement details along with scope to propose the tool. The requested resources wil be dedicated on-premise or will be on demand basis?	Application testing would be under the scope of Vulnerability Management system for vulnerability assessment nad Bug Bounty. The testing would be done on need basis.
27	4. Scope of work for bidder Vulnerability Management Services:	28	The services will include a. Set up a baseline security level for department assets. b. Conduct VAPT and Application Security tests as in when required. c. Bidder has to provide tools / utilities and skilled resources to conduct the respective tests. d. The bidder's (SOC) team has to provide recommendations for closure of findings & provide reports on daily basis till closure. e. Assess the current environment against baseline on periodic basis. f. Ensure that the baseline is maintained on an ongoing basis and hence assets are secured against risks. g. Track the mitigation and coordinate with asset owners for closure of security gaps.	1. Please confirms the number of Apps per year for VAPT and application security test 2. What frequency have these test to be done? 3. Actual closures will be done by application owners. Please confirm a. Kindly clarify whether VAPT and application security assessment will be required to be conducted for all applications listed in Annexure -1 of the RFP b. Kindly confirm whether tools/utilities required for conducting the VAPT and application security tests have to be procured in the name of OCAC. c. Is the bidder's SOC team expected to coordinate with application/infrastructure stakeholders for closure of vulnerabilities ?	As per minimum technical specification and reporting structure already mention in the RFP.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
28	4.1 Pre-Bidding phase Site Survey	28	All Bidders shall be required to survey the proposed CSOC control room site before the submission of the commercials.	1. Due to Ongoing Pandemic its very tough for bidder to go for Site Survey. Hence We request you to kindly allow bidder to quote as per RFP Layouts and specifications. Anything extra post award of contract shall be charged at actual. Please confirm Bidder may visit site to preliminary Survey. However we request you to kindly limit the scope of work to false ceiling, lighting, glass and gypsum / plywood partition, flooring, access control, fire safety and command centre furniture as per given layout. 2. Due do COVID pandemic, we may not be able to visit the site. Request to provide the site layout map with details.	Layout of the site has been provided in the RFP. Bidder may assess the site layout or make a preliminary visit to the site for design and works. Bidder is at its discretion for better design and propose better layout of the CSOC site.
29	4.2 Implementation phase, point no iii	28	The successful bidder in coordination with OCAC shall arrange for necessary clearances including statutory and regulatory which shall enable them to undertake civil, electrical, and mechanical works including building modification.	As building modification is huge task and massive Civil works involved. We request to delete the building modification from bidder's scope.	The civil works involves only interior works and limited civil works. Bidder may visit the site and assess the same.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
30	4.2 Implementation phase	28	ii. Site Preparation. Site preparation structure for CSOC would include false ceiling, lighting, glass and gypsum / plywood partition, flooring, access control, fire safety and command centre furniture. External civil construction may or may not be a part of the scope of the bidder, discretion of developments and future decisions of OCAC. The scope may be revised at a later stage with timely intimation to the bidder. Civil construction inside the identified CSOC space / area would be under the scope of the bidder.	1. We understand that Bidder shall be given fully constructed Building with Proper Doors and Windows along with proper MEP works. Bidder no need to do any modifications outside SOC room. If anything required post award shall be charge at per actual. Also inside SOC Room works includes only false ceiling, lighting, glass and gypsum / plywood partition, flooring, access control, fire safety and command centre furniture. Referred Civil construction inside the identified CSOC space / area would be under the scope of the bidder-only covers false ceiling, lighting, glass and gypsum / plywood partition, flooring, access control, fire safety and command centre furniture. Anything extra shall be mutually discussed at later stage at additional cost. 2. We request to clarify on the	Layout of the site has been provided in the RFP. Bidder may assess the site layout or make a preliminary visit to the site for design and works. Bidder is at its discretion for better design and propose better layout of the CSOC site. The civil works involves only interior works and limited civil works. Bidder may visit the site and assess the same.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
31	4.2 Implementation phase	28	iii. CSOC command centre design, installation and commissioning. The successful bidder in coordination with OCAC shall arrange for necessary clearances including statutory and regulatory which shall enable them to undertake civil, electrical, and mechanical works including building modification, partitioning, installation of electrical component, cable laying etc. at the CSOC site.	1. We understand that Bidder shall be given fully constructed Building with Proper Doors and Windows along with proper MEP works. Bidder no need to do any modifications outside SOC room. If anything required post award shall be charge at per actual. Also inside SOC Room works includes only false ceiling, lighting, glass and gypsum / plywood partition, flooring, access control, fire safety and command centre furniture. 2. As per our understanding and experience of projects like SOC, SDC, SWAN, responsibility of obtaining necessary clearances including statutory and regulatory lies with the client. Therefore, we request OCAC to kindly remove this clause from the scope of bidder.	Layout of the site has been provided in the RFP. Bidder may assess the site layout or make a preliminary visit to the site for design and works. Bidder is at its discretion for better design and propose better layout of the CSOC site. The civil works involves only interior works and limited civil works. Bidder may visit the site and assess the same. Bidder to make all assessments as per layout / site visit. No additional cost would be borne by OCAC unless any additional change / modification in the current site / layout is proposed from OCAC.
32	4.2 Implementation Phase , IV.	29	iv. Design, supply, installation, commissioning for IT and Non-IT 14. Infrastructure for CSOC: The successful bidder should carry out: complete procurement, supply, installation and commissioning of required IT, Non-IT, and civil infrastructure at all the designated locations of the CSOC as identified.	We request you to kindly share the number of designated locations of the CSOC in detail.	1. All major SOC solution would be installed at SDC. 2. Limited solutions e.g: UPS, RACK, CCTV, L2 switch, Router, etc. would be installed at SOC command centre. 3. Log management appliance in pairs would be installed at SDC, SWAN and State IT centre. 4. One Anti-APT solution would be installed at State IT centre.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
33	4.2 Implementation Phase , IV.	29	iv. Design, supply, installation, commissioning for IT and Non-IT Infrastructure for CSOC: Bidder should take care of Insurance against the material loss.	We request you to kindly clarify on the insurance against the material lost. Is the bidder responsible to buy the insurance The bidder requests the following modifications: Please note that the bidder will take care of Insurance against the material loss till the time of delivery at customer premises only. After the items are delivered, the purchaser bears the responsibility to take insurance cover of the items delivered	The bidder to comply as mentioned and defined in the RFP document.
34	4.2 Implementation Phase , IV.	29	v. All components of CSOC must support scalability with adequate licensing, accessories and modules to provide continuous growth to meet the requirements and demand of various departments.	1. Excess licenses / enhancements in features /functions may be at additional cost as agreed. Please confirm.	Any cost implication for additional licenses other than proposed in the RFP would be borne by OCAC.
35	4.2 Implementation Phase	29	v. Bidder should analyze and study the current departmental infrastructure located at OCAC and Secretariat and provide the solution for migration.	Please share the migration requirements to integrate existing dept and security IT infra with proposed CSOC infrastructure. Kindly share the existing asset details and hardware count of OCAC site which are not listed itemwise. We request to clarify that is this activity related to roadmap for migration? or executing migration?	Scope of the bidder is to provide the feasibility for migration if any as per any future requirement in terms of SOC services.
36	4.3 (9)	30	9. Successful bidder will be responsible to store logs in industry standard solution and format for extraction and sharing with other solutions/ agencies.	We request to clarify on the industry standard to be followed to store logs.	Bidder to assess and propose solution.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
37	4.3 (14) Operation and Maintenance phase	30	The services and solutions in scope should be designed with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime and availability.	1. Request please elaborate the SLA for solution. Is the requirement of redundancy applicable to each technology provider? 2. Router quantity given in SOR is single and to meet the redundancy, uptime and SLA requirement, Router should be in HA. Please update the SOR with two routers. 3. Request please elaborate the SLA for solution. Is the requirement of redundancy applicable to each technology provider? 4. As bill of material is already provided in the RFP, we request you to clarify that the bidder is allowed to quote additional components to achieve adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime and availability.	Redundancy should be planned by the bidder considering the BoM mentioned in the RFP.
38	4.3 Operation and Maintenance phase	30	The successful bidder should provide 24 x 7 x 365 operating and maintaining services for a period of 4 years from the date of Go Live for CSOC.	How many seats per shift? Kindly clarify	Details have been provided in Section 8.1 of the document. Bidder may assess and plan likewise.
39	4.3 (17)	31	Engage at least 15 personnel from OCAC / department for the training sessions. Feedback of each attendee to be taken and shared with OCAC.	1. We request OCAC to specify the scope of this training session, the frequency and the timeline for 15 personnel.	Details have been provided in Section 8.1 of the document. Bidder may assess and plan likewise.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
40	4.3 (16)	31	Training to OCAC officials (designated by OCAC) and upgradation of CSOC personnel on IT infrastructure, SLA management, various CSOC related polices, etc.	We request you to kindly clarify on the below: As per our understanding bidder must provide training to 15 personnel from OCAC / department only once. Please confirm.	Trainings to be held annually.
41	4.4 Partial Acceptance Test	31	Partial Acceptance Test	We request to clarify on the percentage of completion to achieve PAT. The bidder needs more clarity on PAT and FAT	Partial acceptance test shall be done for every scope of work under the successful bidder seperately at different intervals or completion of each scope.
42	4.5 - Final Acceptance Testing (FAT)	31	The acceptance of the Data Centre including DC site in accordance with the requirements shall be conducted	The bidder needs more clarity on PAT and FAT	Final acceptance test shall be done for the whole scope of work of the bidder after commissioniong.
43	4.5 - Final Acceptance Testing (FAT) Point 6	32	6. The successful bidder shall be responsible for the security compliance of the infrastructure and network before the final acceptance test.	Q1:We request OCAC to detail out the security compliance requirements of the infrastructure and network. Q2:We request OCAC to clarify on the "security compliance" requirement by sharing information on criteria used for verifying the security compliance or what will be the criteria to be considered by Bidders for the security compliance.	Bidder to asses as per applicable inductry standards and market best practices.
44	4.5 - Final Acceptance Testing (FAT)	32	Final Acceptance Testing (FAT): 5. The successful bidder will arrange the test equipment required for performance verification and provide documented test results.	We request you to clarify on the test equipment here. Is it other than the bill of material mentioned in the RFP?	For FAT period, if any additional tool is required, the cost would be borne by the bidder. We understand bidder would already have a tool in place to provide compliance of the solution proposed.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
45	5.1	33	Project high-level architecture	We request OCAC to kindly clarify on below: As OSDC and OSWAN are on the same premises where CSOC will be established. Can the bidder terminate the connectivity to OSDC and OSWAN from the core switch instead of router?	1. All major SOC solution would be installed at SDC. 2. Limited solutions e.g: UPS, RACK, CCTV, L2 switch, Router, etc. would be installed at SOC command centre. 3. Log management appliance in pairs would be installed at SDC, SWAN and State IT centre. 4. One Anti-APT solution would be installed at State IT centre.
46	5.2 Site Layout	33	The CSOC site would be prepared as the specifications provided at First floor, OCAC Tower, Acharya Vihar, Bhubaneswar, Odisha.	Please provide the Auto Cad Drawings of the Proposed Room. Also we need the Total Floor to Floor Height	Would be shared with the successful bidder.
47	5.2 Site Layout	33	Layout	The distance between Video Wall and the 1st Row is shown as 1.5 Mtrs. We feel the same is less and it should be at least 3.0 Mtrs as per Ergonomics and better view of the Human Eye. The Area allocated for SOC Room of 821 Sq. ft is very less and in our views. We'll require at least 1500 Sq.ft of Space to meet the RFP requirement. Kindly clarify	The floor layout is for 1500 Sq.ft.
48	5.2 Site layout	35	Note: 6. The bidder has to carry out any civil construction as required at the site for building up Odisha Cyber SOC.	Kindly delete this clause as its very generic. Kindly help us with exact scope in terms of Civil Construction.	Layout of the site has been provided in the RFP. Bidder may assess the site layout or make a preliminary visit to the site for design and works. Bidder is at its discretion for better design and propose better layout of the CSOC site. The civil works involves only interior works and limited civil works. Bidder may visit the site and assess the same.
49	5.2 Site Design	36	Aspirating smoke detection, water leak detection, rodent repellent, CCTV, access control system	Aspiration Smoke Detection and Water Leak Detection needs to be considered for all Rooms or only for Server Room and UPS Room.	It should be proposed for all rooms.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
50	5.4	36	False flooring for Command Centre	Design details not mentioned 1. Raised false flooring in which area , kindly specify dimension 2. Stone flooring in which area, kindly specify rooms and total floor area to be covered by stone. 3. Carpeting in which area , kindly specify the are for which carpet is required.	Bidder to assess and propose the design for SOC site.
51	5.3 Site Design	36	After implementation of the civil works, the bidder has to obtain relevant certifications for the site and share the same with OCAC.	Kindly clarify what all certificates are needed for completion as it a space in already built up building	Bidder to share with OCAC the certificates as mentioned in Section 5.4 of ther RFP document under various scope of work and design items. Any additional certificate which the bidder may asess and seem fit to the work done, may be shared with OCAC.
52	5.4	37	2. Italian Marble / Composite stone flooring	Design details not mentioned	Bidder to assess and propose the design for SOC site.
53	5.4	37	3. Carpet flooring	Design details not mentioned	Bidder to assess and propose the design for SOC site.
54	5.4	37	Partitions and Panelling	Detail description for partion & detail description for panelling & Qty. individualy mentioned which type of partion & panelling is required.	Bidder to assess and propose the design for SOC site.
55	5.4	38	Double leaf glass door	Size & Qty. not mentioned	Bidder to assess and propose the design for SOC site.
56	5.4	38	Fire rated steel door	Size & Qty. not mentioned	Bidder to assess and propose the design for SOC site.
57	5.4	38	Fire rated toughened glass door	Size & Qty. not mentioned	Bidder to assess and propose the design for SOC site.
58	5.4	39	Metal Baffle ceiling	Qty. details not specified. Design & Drawing details not Specified	Bidder to assess and propose the design for SOC site.
59	5.4	39	Designer Acoustic false ceiling	Qty. details not specified. Design & Drawing details not Specified	Bidder to assess and propose the design for SOC site.
60	5.4	39	Curvilinear or designer ceiling	Qty. details not specified. Design & Drawing details not Specified	Bidder to assess and propose the design for SOC site.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
61	5.4	40	Site Civil & Non IT Works - FURNITURE 1. Control Desk (H x W x D = 750mm X 9478mm X 900 / 1050 mm)	Design Not mentioned	Bidder to assess and propose the design for SOC site.
62	5.4	41	Site Civil & Non IT Works - FURNITURE 2. Manager Table (H x W x D = 750mm X 1800mm X 800mm)	Design Not mentioned	Bidder to assess and propose the design for SOC site.
63	5.4	42	Site Civil & Non IT Works - FURNITURE 3. Meeting Room Table (H x W x D = 750mm X 2700mm X 1050mm)	Design Not mentioned	Bidder to assess and propose the design for SOC site.
64	5.4	42	Site Civil & Non IT Works - FURNITURE 4. Reception Table (H x W x D = 1000mm X 1500mm X 700mm)	Design Not mentioned	Bidder to assess and propose the design for SOC site.
65	5.4	42	Site Civil & Non IT Works - FURNITURE 5. Command centre chair - 16, Meeting room chair / Visitor Chair - Chair for Office - 6; Manager Chair - 1	OEM/ Make not Specified	Bidder to assess and propose the design for SOC site.
66	5.4	42	Site Civil & Non IT Work 7. Sofa Set	Design, Detail and Model No. along with Sitting Capacity	Bidder to assess and propose the design for SOC site.
67	5.4	42	Site Civil & Non IT Work 7. Coffee Table	Design, Detail not specified	Bidder to assess and propose the design for SOC site.
68	5.4	42	Site Civil & Non IT Work 9 - Storage Unit	Design and Finish Detail not Specified	Bidder to assess and propose the design for SOC site.
69	Electrical	43	Supply, storing, handling, laying, testing and commissioning of 1100 Volt grade XLPE insulated and sheathed aluminium conductor armoured cables, ISI marked, ncluding providing required gap between adjacent cables (minimum one cable dia.) including providing identification tags in shaft/ cable trays etc. complete as per	Please confirm the Location of the 2 Breakers and the Rating Availaible for the Bidders to tap the Power for the Entire SOC Area.	Bidder to assess and propose the design for SOC site.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
70	5.4	43	Site Civil & Non IT Work Electrical Wires, Switches & Conduits for ceiling and floor lights	Detail electircal design & drawing not Specified Kindly confirm that raw power supply and DG set power backup will be provided by OCAC.	Bidder to assess and propose the design for SOC site.
71	5.4	43	Site Civil & Non IT Work Passive Cabling with components	Detail electircal design & drawing not Specified	Bidder to assess and propose the design for SOC site.
72	5.4	43	Site Civil & Non IT Work Distribution Board with Electrical MCB complete	Detail make & models not specified, Qty. details not specified. Specification Not Specified	Bidder to assess and propose the design for SOC site.
73	5.4	43	Site Civil & Non IT Work Modular switch board with switches and sockets for Desk with complete wiring	Detail make & models not specified, Qty. details not specified. Specification Not Specified	Bidder to assess and propose the design for SOC site.
74	5.4	44	Site Civil & Non IT Work Air Conditioning	No. of AC Outlet not specified, Ducting size not specified	Bidder to assess and propose the design for SOC site.
75	5.4	44	Site Civil & Non IT Work General LED Ceilling lights	Detail make & models not specified, Qty. details not specified.	Bidder to assess and propose the design for SOC site.
76	5.4	44	Site Civil & Non IT Work Circular / Dimmable LED lights	Detail make & models not specified, Qty. details not specified.	Bidder to assess and propose the design for SOC site.
77	5.4	44	Site Civil & Non IT Work LED strips	Detail make & models not specified, Qty. details not specified.	Bidder to assess and propose the design for SOC site.
78	Air Conditioning	44	The bidder should to visit the site prior to bidding to assess the air conditioning input duct and dimensions to plan propose likewise. The bidder is required but not limited to perform the following activities: i. Supply and Installation of AC duct work from the AHU mouth for the entire area of SOC	1. We understand we have to use the Existing AHU for the Cooling of the Entire Area. We need the HVAC Schematic and the Rating of the Chiilers etc. installed for the Building to understand how the solution needs to be proposed. 2. We also need to understand what Redundancy is planned as SOC Area will require redundnacy for 24 x 7 Operation.	Bidder to assess and propose the design for SOC site.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
79	6.2	46	Paralleling Operations – The output of all the UPS systems would be directly connected at the load distribution panel through individual circuit breakers (part of the distribution panel). The load at the output would be shared equally by all the UPS systems. The paralleling control mechanism would be available with individual UPS. There would not be any single point of failure which can lead to collapse of all the UPS systems	Please confirm the quantity of UPS to be considered in parllel configuration for one set.	2 nos. of 20 KVA to operate in parallel.
80	6.2 UPS	46	24. Minimum 60 minutes back-up on full load	As DG will start in within 3-5 Minutes so we feel 30 Minutes on Full Load is Sufficient as this increases the Opex & Capex Cost.	UPS back-up for 60 minutes applicable.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
81	6.9	52	The Rear Projection Modules must be based on Single Chip DLP,Full HD (1920X1080) Native, Rear Projection technology. The displays shall utilize RGB Laser having different laser bank for different colors respectively without any moving part.	Please note the Video wall mentioned here is that of rear projection or traditional DLP based Video wall which is a niche technology which only few O.E.Ms make and its not widely accepted. If we look at the total market share of Video wall then we will find that only 2% of market share is comprised of DLP Videwalls and majority is comprised of LCD based Video walls.We can also offer the latest trend in market known as Active LED which is ideal for the mission critical application like this in which there is a Bezel less screen with very high picture clarity and brightness.DLP and rear projection systems are very bulky and traditional whereas the LCD/Active LED are much compact and optimises the room usage.We therefore request you to allow LCD based Video walls or Active LED as these are more reliable than rear projection and more widely accepted than them.By incorporating rear projection videowalls this case is	The criteria is kept as per the criticality of the solution and requirement.
82	6.8	52	Equipped with an IPS panel with 178/178 viewing angle	Please make it Vertical allignment as IPS is propreitory to some specific OE.Ms and VA (Vertical Allignment) ensures better static Contrast ratio.	The criteria is kept as per the criticality of the solution and requirement.
83	6.8	52	Have maximum response time of 4 milliseconds	Please note 4 ms is not a standad for professional displays used for business usage.Request you to please make it 8ms which is as per market standrad.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
84	6.9 Display – Video wall with controllers and speakers / Functionality /Video wall	52	The system should have a continuous duty cycle of 24/7 for color calibration and brightness uniformity using automated software via external server and should also support manual override function and feature on demand.	Please remove external Server from this point. Justification: 1. It should be a inbuilt auto correction system to ensure enhanced system performance and long life without external intervention to monitor various parameters of the system and automatically performs real time adjustments to deliver the optimum performance and reliability needed for a 24x7 system. 2. Video wall shall be accessible over the IP through browser / server architecture based software tool for monitoring, controlling and diagnostic purpose. Adding External server will add cost.	The criteria is kept as per the criticality of the solution and requirement.
85	6.9 Display – Video wall with controllers and speakers / Functionality / Video controller	53	Regulatory Compliance : UL, CB, BIS,FCC,CE ,IEC 60950, IEC 62368	Please change to : Regulatory Compliance : BIS which is mandatory for India . As per new Public procurement guidelines of ministry of government India international ceritificate are not mandatory in the tender.	The criteria is kept as per the criticality of the solution and requirement.
86	6.9 Display – Video wall with controllers and speakers / Functionality / Software	54	Integrated Embedded & External Audio formats with Audio decoding of video streams also possible Software also supports UMD, IDC, Source name, Time (time zone aware), Date, text, Logo, Message Ticker, Source Status	Please remove this clause. Justification: This is specific to one OEM. Please remove this to increase OEM participation.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
87	6.9 Display – Video wall with controllers and speakers / Functionality / Software	55	Supported sources: Analog & digital / streaming video, Analog (RGB) and Digital (DVII) Sources, Network desktops, Network multi-channel workstations and applications, Internet & internet sources, Embedded & external audio formats, Localization	a. Please confirm no. and type of analog (RGB) and digital DVI inputs. b. For streaming video Kindly Confirm: 1. Is video decoding in our scope? 2. How many cameras to be decoded & at what resolution? 3. How many cameras would be seen simultaneously on the video wall? c. how source will have Embedded & external audio formats ? d. What you mean by localization ? please clarify	The criteria is kept as per the criticality of the solution and requirement.
88	6.9 Display – Video wall with controllers and speakers / Technical Specifications/Video wall	55	> 700 Nits on screen	Suggested specifications: Brightness of Cube : Minimum 400 nits or higher and should be adjustable for lower or even higher brightness requirements. Justification: 700 nit brightness will be too bright for the control room operator and will cause unnecessary strain to operators eyes	The criteria is kept as per the criticality of the solution and requirement.
89	6.9	55	Laser with lifetime minimum 100000 hours	Laser technology cubes are only used in rear projection or DLP videowalls. We recommend you to please go for LCD or Active LED based Videowalls.	The criteria is kept as per the criticality of the solution and requirement.
90	6.9	55	Projector is equipped with Automatic motorized alignment no manual alignment needed	Rear projection is asked for which is a bulky technology and requires lots of space.Request you to consider LCD based Video walls which are much lighter and slim and no bulky/motorised equipments needed.Its compact and ideal for such usage.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
91	6.9	55	Should be IP6X certified by third party laboratory	This is not required as this is a mission critical usage and always has a Conditioned room environment where exposure to outside dust doest exist.	The criteria is kept as per the criticality of the solution and requirement.
92	6.9	55	Serviceability should be rear	Please note that in rear projection Videowalls cubes ; 500mm of depth space is required which is quite some space for rear servicability and for optimising space its always recommended to go for LCD Video walls whose depth is very less and always less than 90mm including sceen and frame.That is why LCD walls are always very compact and helps to optimize space.	The criteria is kept as per the criticality of the solution and requirement.
93	6.9	55	Screen Gap should be Less Than 1mm	Please make Screen gap 0.88mm Bezel to Bezel which is better.In LCD we have 0.88mm Bezel to Bezel and in Active LED its totally Bezel less and provide continous screen which is best suited for such mission critical appliction.	The criteria is kept as per the criticality of the solution and requirement.
94	6.9	55	Power consumption should be Less than 200 watt in Normal/Typical mode	We can provide 96W typical in LCD Videowall which is much better than what is asked in tender.	The criteria is kept as per the criticality of the solution and requirement.
95	6.9	55	Heat Dissipation should be Less than 800 BTU/hr	We can provide 488 BTU/hr which is half than what is asked for and much better.	The criteria is kept as per the criticality of the solution and requirement.
96	6.9	55	System shall operate properly under 10ºC to 40ºC Temperature , Humidity - 20%-80%	Please make Humidity 10 to 80 degree which is standard.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
97	6.9	55	All cubes shall of 70" diagonal size and optimized to work in a multi-screen arrangement (4 X 2)	Please also note here 70 inch Panel size is asked for which again is non standard and available to only few O.E.Ms restricting others to participate.In Video wall domain the standard size available world wide is 55 inch each panel.We can configure any size with 55 inch so we can match the configuration or dimension required in this tender.We can also offer Indoor Active LED which is totally Bezel less which is ideal for mission critical application like this.This is best suited for such applications where in higher clarity for showing data content is required.Samsung has both LCD(55 inch) and Active LED technology which is Bezel less and are best suited for such critical applications offering very High picture clarity.	The criteria is kept as per the criticality of the solution and requirement.
98	7.1 Security Orchestration Automation & Response (SOAR)	57	3. SOAR platform should support common methods of data ingestion, such as syslog, database connections, APIs, email and online forms, as well as common data standards such as CEF, Open IOC, STIX/TAXII, etc.	SOAR platform should support common methods of data ingestion, in the form APIs, email and TCP listeners. Common data standards supported are CEF, Json, XML	The criteria is kept as per the criticality of the solution and requirement.
99	7.1 Security Orchestration Automation & Response (SOAR)	57	8. Solution must be able to support creation of incidents via API, Web URL, SIEM, Ticketing system, etc.	SOAR supports creation of incidents via API, Web URL, SIEM, Threat Intel Feeds, Emails.	The criteria is kept as per the criticality of the solution and requirement.
100	7.1.9	57	Should support codify process like linear-style playbooks, flowcontrolled workflows or run books.		The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
101	7.1 Security Orchestration Automation & Response (SOAR)	57	12. Should have capability to provide simulation environment to test playbooks without relying on access to real environment.	How many Authorinzed Users or Concurrent users would need to access the SOAR product for administration? Only one type of users i.e. Authorized or Concuurent users would be able to access the SOAR console.	The criteria is kept as per the criticality of the solution and requirement.
102	Security Orchestration Automation & Response (SOAR)	57-59	Requirement Description	Please provide the details of the solution/Components which are to be integrated with SOAR solution.	The criteria is kept as per the criticality of the solution and requirement.
103	7.1 Security Orchestration Automation & Response (SOAR)	58	Should the capability for different forms of threat hunting, while actively looking for attacks and patterns that may not have been detected through automated methods.	Request to provide additional information around this feature. We understand that from this feature the ask is to have capability to investigate more around the artifact to enable analyst by having additonal insight on the incident	The criteria is kept as per the criticality of the solution and requirement.
104	7.1 Security Orchestration Automation & Response (SOAR)	58	Should be able to integrate with all devices irrespective of the OEM or manufacturer.	SOAR technology support integration with different thirdparty product using tehnologies such as Rest API , Python , JS , email escalation etc. For any integration the support is required on both technologies. It is thus requested to re-phrase the same as " The solution should integrate with all devices which support integration using technologies such as Rest API , python , JS , email etc. Also, reques to share the comprehensive list of devices planned to be integrated initially with this solution.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
105	7.1 Minimum technical requirement Security Orchestration Automation & Response (SOAR) SI No-20	58	The following additional features should be available in the SOAR solution: - Phase and objective tracking - Detailed task tracking, including assignment, time spent and status - Asset management, tracking all physical and virtual assets involved in the incident - Evidence and chain of custody management - Indicator and sample tracking, correlation and sharing - Document and report management	We are request to modify the Clause as "The following additional features should be available in the SOAR solution by integration with CMDB and ITSM tool: - Phase and objective tracking - Detailed task tracking, including assignment, time spent and status - Asset management, tracking all physical and virtual assets involved in the incident - Evidence and chain of custody management - Indicator and sample tracking, correlation and sharing - Document and report management	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
106	7.1 SOAR, 33		Should support at least four analysts' user accounts and support scalability for increase in the number of analyst accounts.	SOAR solution is accessed by not just analysts but also security management and leadership teams like CISO, SOC Manager, Complaince Team, IT remediation teams. So the solution should provide capability for other users other than analysts to be able to login, view and comment on ongoing incident tasks and investigations. This feature is very important for any type of incident collaboration and management oversight of SOC function. So we request to add/modify below point to Should support at least four analysts' user accounts and 4 management level oversight accounts. And support scalability for increase in the number of analyst accounts.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
107	7.1 Minimum technical requirement Security Orchestration Automation & Response (SOAR) SI No-44	59	Should be able to integrate existing SIEM /ESM solution irrespective of the OEM and version.	1. In Page 59, RFP asked to upgrade the existing SIEM solutions or propose a new SIEM solution. Also in RFP page No-27, under "Security Product Management" OCAC wants a centralised management of security products to have tight control on the security rules. Therefore we request to modify the clause as "Solution should be tightly integrate with SIEM, SOAR, UEBA, ML, DLP in a single platform as and when required for centralised management of security products and have tight control on the security rules" 2. SOAR technology support integration with different thirdparty product using tehnologies such as Rest API , Python , JS , email escalation etc. For any integration the support is required on both technologies. It is thus requested to re-phrase the same as " The solution should integrate with all devices which support integration using technologies such as Rest API .	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
108	7.1 Security Orchestration Automation & Response (SOAR)	59	Solution should not have any restriction on the number of response actions and creation of playbooks.	Please provide details of number of concurrent users that shall be accesing the solution at any point of time. The industry practise to have atleast 3-4 indiviual manned at such solution at all point of times.As per best practise one analyst can manage at max 4-5 incident/day thus requiring around 40 actions/day assuming 8 actions per incident. Based on this calculation around 160 action/day and a total of 5000 Action/month would suffice the requirement. You can factor additional 40% considering spikes and burst or some breach. It is thus request to allow OEM to factor the solution with 7000-8000 actions per month as part of the BOQ. Enabling fixed number of actions keeping in mind the burst will help the organization optimize the the solution making it more cost effective.	Modification: "Solution should have capability for at least 1000 number of response actions per day of the whole span of the project."
109	7.2 Log Management appliance 7.3 Security Information and Event Management (SIEM)	59-63	Requirement Description	Please confirm , the existing security components (Logs Management Appliance and SIEM) deployed in OSDC (Odisha Sate Data centre) is fully compliant on all the technical requirements as mentioned in Section 7.2 and Section 7.3	Bidder to assess as per details of existing infrastructure provide in the RFP document and propose accordingly.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
110	7.2 Log Management appliance 7.3 Security Information and Event Management (SIEM)	59	GENERIC	Please provide the list of devices/solutions/components which are currently integrated with existing SIEM solution Please also provide list of devices/solutions/components which will be integrated with SIEM solution in future.	Would be shared with the successful bidder.
111	7.2 Log Management Appliance Note 2.	59	The bidder is provided with an option to either upgrade the existing solutions & utilize for SOC or may propose a new SIEM solution along with logger appliances, however the existing solution shall be integrated with SOC.	1. The term "Logger" is specific an OEM. Proposed solution has SIEM, SOAR, UEBA feature in a single Big Data Analytical solution and has the in built capability of log collection module. 2. In case bidder chooses to integrate with the exiting SIEM components, can you please confirm that these components are not getting EOL or EOS for the entire 4 years. Also, who would be responsible for renewing the support of these existing SIEM componenets? 3. This is a properiatory clause. In case bidder is proposing New SIEM, it should integrate with the proposed SoC components and not the existing solution. 4. In the Log Management feature OCAC want collection and analysis data along with online retention of log data for 90 days	Log managemet appliance should be considered by bidders when proposing solution for the RFP. The solution architecture and nomenclature may vary, but the minimum technical requirements should be met by the solution.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
112	7.2 Log Management appliance	59	The log management appliance should be capable and compatible to integrate with the below devices: 1. Security Information and Event Management / ESM a. Make: HPE ArcSight	1. Do you have an existing HP Arcsight solution & do you want to continue with it or intend to procure a new SIEM solution. 2. Is the existing Arcsight solution deployed in HA ? What will be the online / offline retention log period to be factored? Please share no. of users /endpoints that is considered for existing UEBA solution?	Bidder to assess as per the details provided in the RFP and propose accordingly.
113	7. Minimum technical requirement (IT assets)	59	7. 2 Log Management	In the Log Management feature OCAC want collection and analysis data along with online retention of log data for 90 days.	All data should be stored within the device / solution for at least 90 days.
114	7. Minimum technical requirement (IT assets)	59	7.2 Log Management. Forward logs to 3rd party analysis tools or fetch data from SSB via its REST API	Could you please let us know which third party analysis tools do OCAC need the logs from logger to be forwarded to?	Would be shared with the successful bidder.
115	7.3 Security Information and Event Management (SIEM)	61	General	Current EPS requirement is 21000 (peak) and the same shall be scalable to add additional 14000 EPS (Peak) in future . Please confirm	Bidder may refer the minimum technical specification for SIEM and Log Management appliance and propose accordingly.
116	7.3 Security Information and Event Management (SIEM)	61	2. Solution should encompass log, packet and end point data with added context and threat Intelligence.	Solution should encompass log, packet and end point data with added context and threat Intelligence by integrating with requisite event sources.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
117	7.3 Security Information and Event Management (SIEM) Sr. No 4	61	7.3 There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department. The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required	We request OCAC to kindly specify the number of devices to be supported & monitored as it is dependent on EPS procured and has a cost implication around it.	The details have been mentioned in the RFP document.
118	7. Minimum technical requirement (IT assets)	62	7.3 Security Information and Event Management (SIEM) 23. It should be able to handle a burst of 1.25 times of the sustained EPS in real time at any given point in time without any drop or queuing of events.	1. QRadar Hardware/Virtual appliances normally can handle burst rates at least 50% greater than the appliance's stated EPS and FPM capability, and can store up to 5GB in the temporary queue. Could you please confirm if this fulfills OCAC's SIEM burst handling requirements?	Bidder to assess the requirement mentioned in the RFP and propose accordingly.
119	7. Minimum technical requirement (IT assets)	62	7.3 Security Information and Event Management (SIEM)	Do OCAC want a DR solution for SIEM running in parallel or a Cold Standby SIEM which can be powered on when the SEIM at the primary DC goes down?	Bidder to assess the requirement mentioned in the RFP and propose accordingly.
120	7.3 Security Information and Event Management (SIEM)	63	27. Should support storage and archiving of data and reports as per requirement.	Please provide the log retention policy for both online and offline storage , kindly also provide the storage size provisioned and occupied for existing SIEM solution.	Bidder to assess the requirement mentioned in the RFP and propose accordingly.
121	7.4 Anti – Advanced Threat Persistent (Anti – APT)	63	General	Please provide the scope for Anti-APT solution and also the list of solution which are to be integrated with Anti-APT solution.	Details would be provided with the successful bidder.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
122	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 5	63	Enhance security intelligence similar to NGFW and NGIPS "learn" from attacks	For OCAC to have a defense in depth strategy by having differnet layers of security by different OEMS's so as to to adhere to the dual incident monitoring design principle. (Similar has been asked in the Intelligence feeds clause as well). Suggest to rephrase this clause as below The solution should have no dependency on any other network device (e.g. firewall, IDS/IPS, security gateway, etc) for its functioning. The capability should not be bundled as a part of an existing UTM or integrated security solution and should be capable of working in standalone mode.The propsoed Anti-APT should be of different OEM from Firewall & IPS deployed at OCAC Odisha.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
123	7.4 Anti - Advanced Persistent Threat (Anti-APT). Clause 7	63	Use specialized detection engines, correlations rules, and custom sandboxing to detect all aspects of an advanced persistent threat, not just malware.	Having custom sanboxing will increase the complexity and overhead for OCAC and corelation rules should be in the scope of SIEM which is part of this RFP. The Images in Sandbox must be pre-instrumented built, maintained, and delivered by the OEM to product/solution deployed in order to avoid any complexity of installing applications and maintaining VM's by OCAC Odisha" This clause should be rephrased as below "Use specialized detection engines using static & dynamic analysis to detect all aspects of an advanced persistent threat, not just malware."	The criteria is kept as per the criticality of the solution and requirement.
124	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 18	64	Capable of unlocking of password-protected files and Zip files	Nested ZIP archives causes well-known attack due to known unpacking attacks, such as zip bombs and quines, including 42.zip so request you to remove this clause.	The criteria is kept as per the criticality of the solution and requirement.
125	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 20	64	Supports SPAN port or port mirroring configuration	As it has been asked in point 37 "The solution should support both inline and out of the band mode." Kindly consider the clause 37 in order to avoid confusion and overlapping duplication.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
126	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 21	64	Able to integrate with multiple devices and analyze all information in parallel	Please clarify as integration of Anti-APT solution & devies with SIEM tool has been asked as a separateley at clause 48. Kindly remove this clause.	The criteria is kept as per the criticality of the solution and requirement.
127	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 29	64	The solution should be able to inspect and block all network sessions regardless of protocols for suspicious activities or files at various entry/exit sources to the client's network.	Please clarify, entry/exit sources in the client's network. Kindly ammend this clause as below "The solution must support an inline blocking mode. TCP Reset is not an acceptable form of blocking.It must stop infection, compromise and intrusion phases of the cyber-attack kill chain by identifying malicious exploits, malware and command and control (CnC) callbacks. It must extract and submits suspicious network traffic to the sandboxing engine for a definitive verdict analysis."	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
128	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 31	64	The solution should be able to identify malware present in network file shares and web objects (QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, ico, jar, jpeg, jpg, mov.) and able to quarantine them.	Please clarify as below there is duplicacy of the clause (33) similar to this clause to make it a single clause. Kindly ammend this clause as below The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm to prevent advanced Malware and Zero-day attacks.	The criteria is kept as per the criticality of the solution and requirement.
129	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 32	64	The solution filter must support network action set such as Block (drop packet), Block, Permit, Trust, Notify, Trace, Rate Limit and Quarantine & must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic	Please clarify, As malicious communication to a CnC should never be permitted,Trusted,Notified these should always be blocked as a practice. Kindly ammend this point as below "The solution must support an inline blocking mode. Also TCP Reset is not an acceptable form of blocking."	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
130	7.4 Anti - Advanced Persistent Threat (Anti-APT). Clause 33	64	The solution should be able to identify zero-day malware present in file and web objects (Adobe Flash File, Java, Microsoft Office Files .doc .docx .ppt .pptx .xls .xlsx, .pdf, rar, dll, sys, tar, exe, zip, bzip, 7zip, ink, chm, swf etc.) and should have ability to interrupt malicious communication.	As per the suggestion against point 31 "Suggest to ammend this clause as below there is duplicacy of the clause (31) similar to this clause to make it a single clause. The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm to prevent advanced Malware and Zero-day attacks."	The criteria is kept as per the criticality of the solution and requirement.
131	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 35	65	Solution should identify spear phishing email, zero day malware and ransomware attacks in email and should quarantine or block suspicious email messages before reaching user/ mail server.	Kindly to ammend this clause as below as Email APT is not in the scope of this RFP. "Solution should support extensive metadata protocols including the following protocols: FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
132	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 36	65	The solution should support Sandbox test environment which can analyse threats to various operating systems, browsers, databases etc.	Please clarify this point, as a best practice databases are not recommended to be run in the sandbox environment as this would choke the resources. Kindly rephrase this point as below as the "The solution should support Sandbox test environment which can analyse threats to various operating systems, application & service packs versions etc."	The criteria is kept as per the criticality of the solution and requirement.
133	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 38	65	The solution should be able to detect and prevent bot outbreaks including identification of infected machines.	Please clarify, As this point is focussed on the bot outbreaks it should be addressed using the endpoint security. Kindly remove this clause.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
134	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 39	65	The solution should be appliance based with hardened OS. No information should be sent to third party systems for analysis of malware automatically.	This clause is in contradiction to clause 44. Kindly ammend this clause as below "The solution should be a physical applaince based Virtual Execution or Sandboxing component should be secure hardened hypervisor and should not be from list of Commercially Available Off The Shelf (COTS) hypervisor like VMWARE,HYPERV,CITRIX ,Oracle etc since advance malware can easily make out when executed in COTS based hypervisors do not show behaviour leading to poor detection & False Negatives . This is critical hence detection engine should be resistant to VM evasion techniques used by advance malware in APT attacks.	The criteria is kept as per the criticality of the solution and requirement.
135	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 41	65	The solution should be able to share malware information/ zero day attacks knowledge base with deployed appliances.	Please clarify as "Threat Intelligence" has been asked separately as part of this RFP. Kindly remove this clause.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
136	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 42	65	The solution should be able to capture packets for deep dive analysis.	Please clarify as packet captures are provided by Anti-APT solution for the corresponding alerts generated by the anti-APT solution. Please clarify else it should be in the scope of the separate packet capture tool. Kindly ammend this point as below " The solution should be able to capture packets for deep dive analysis for the alerts generated by the Anti-APT solution"	The criteria is kept as per the criticality of the solution and requirement.
137	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 46	65	Dashboard should have the feature to report Malware type, file type, CVE ID, Severity level, time of attack, source and target IPs, IP protocol, Attacked ports, Source hosts etc.	Please clarify, As different information is availabe in the different widgets of dashboard is the expectation is to have all the information in a single screen ? As different OEM solution would provide Clause desired information in different widgets & reports. We suggest to rephrase this clause as below "The solution should provide a Dashboard that offers real time threat visibility and attack characteristics"	The criteria is kept as per the criticality of the solution and requirement.
138	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 47	65	The solution should generate periodic reports on attacked ports, malware types, types of vulnerabilities exploited etc.	Please clarify, as this point is focussed towards reporting it should be mention the reporting formats also.Kindly ammend this point as below The solution shall provide reports in (not limited to) HTML/CSV/PDF Formats. The solution should generate Indicators of Compromise including IPs, port, protocol and domains	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
139	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 59	66	Minimum performance throughput up to 2 Gbps	Please clarify that weather 2 Gbps performance throughput is a really required or change it to 1 Gbps. Considering number of users are 148 (Taken from the RFP page number 133) 1 Gbps will suffice the need. AS per our engagement with IT/ITeS we have seen 1 Gbps will suffice the needs so that OCAC will get benefitted with proper sizing which doesnt gets oversized and overpriced.	The criteria is kept as per the criticality of the solution and requirement.
140	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 60	66	Should be able to store online data for at least 90 days.	As the asked solution is an on-premise solution so kindly ammend this point as below "Should be able to store the logs on-premise for atleast 90 days"	All data as per requirment should be stored within the device / solution for at least 90 days. Any data beyond 90 days period shall be archived in external storage as proposed in the RFP.
141	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 63	66	Supports OS: Win 10 (64-bit), Win 8.1 (64-bit), Win 8 (32-bit/64-bit), Win 7 (32-bit/64-bit), Win XP (32-bit/64-bit), Win Server 2016, Win Server 2012, Win Server 2012 R2, Win Server 2008, Win Server 2003, Android, Mac, Linux	"As per the suggestion given for clause 11 under Anti-APT. Kindly consider so as to remove duplicate points and to avoid overlap."	The criteria is kept as per the criticality of the solution and requirement.

Sl #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
142	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 66	66	Should be capable to add multiple number of monitoring nodes logically.	Please clarify on "monitoring nodes logically". Also kindly ammend this clause as below as existing clause is not clear. "The proposed solution should have the ability to be deployed in the following modes: - inline blocking - inline monitoring and, - SPAN mode. All necessary additional devices, licenses required for such configuration should be quoted as part of the solution"	The criteria is kept as per the criticality of the solution and requirement.
143	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 67	66	Should support scalability in number of ports for expansion.	Please Clarify. Also request to provide the sizing being looked upon by OCAC for Anti-APT solution. As considering number of email users are 148 (Taken from the RFP page number 133) the proposed Anti-APT solution will cater the current and future need as well for scalability.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
144	7.4 Anti - Advanced Persistent Threat (Anti-APT) Clause 69	66	Have maximum MTBF and least MTTR	Request to clarify the point as different OEMS have different MTBF & MTTR for different appliances. Also this is related to applaince hardware failure for which the RMA is to be raised which is part of the proposed solution.	The criteria is kept as per the criticality of the solution and requirement.
145	7.5 Network Traffic Analyser	66	General	Please provide the scope of Network Traffic Analyser , which type of traffic needs to be analysed - Internet , Intranet , protocols to be analysed.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
146	7.5 (2) Network Traffic Analyzer	66	Identify bandwidth hogs down to a user, application or device level.	1. Please confirm whether the activities to determine bandwidth choke are to be manually executed or automated.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
147	7.5 (23) Network Traffic Analyzer	67	Should be able to generate and retrieve reports for a minimum of one year period where online data should be available for minimum 90 days period.	1. Request the buyer to please confirm whether a centralized storage facility will be made available to move snapshot of daily data for archival & reference purpose. 2. The licensing si done on the basis of Network Flows Per Minute. If the Flow Volume Per minute is not known already then we are presuming that OCAC would provide us their IT inventory for us to determine the Flow license. Could you please confirm on this.	All data as per the requirement should be stored within the device / solution for at least 90 days.
148	7.5 Network Traffic Analyzer	67	Should be able to generate and retrieve reports within the appliance	Please Clarify whether its can be Software appliance or Hardware appliance , If Software appliance who will provide the resource and storage	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
149	Network Traffic Analyzer	67	7.5 Network Traffic Analyzer 20. Should include a distributed search engine data-store to ingest various types of textual, numerical, geospatial, structured and unstructured data.	1. Could you please elaborate on this requirement?	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
150	7.5 Network Traffic Analyzer	66	26. Should support for reconstruction of session if raw capture retention is configured.		The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
151	Network Traffic Analyzer	67	7.5 Network Traffic Analyzer 27. Should not require an internet connection in support of any of its capabilities. It should be possible to schedule ingestion of OEM supplied and third-party threat intelligence by importing the update using system console or CLI or scheduling checks with a locally hosted repository.	1. We are presuming that OCAC would be fine with a Network Behaviour and Anomaly Detection solution which is a managed host of the centralized SIEM solution which is be default gets Global Threat Intelligence from the proprietary Threat Intelligence paltform. Network Flow correlation would be able to leverage the Threat Intelligence feeds colelcted by the SIEM.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
152	7.5 Network Traffic Analyzer	67	29. Should support minimum 10 Gbps of throughput performance.		The criteria is kept as per the criticality of the solution and requirement.
153	7.5 Network Traffic Analyzer	67	30. Should support SPAN / port mirroring.		The criteria is kept as per the criticality of the solution and requirement.
154	Network Traffic Analyzer	67	7.5 Network Traffic Analyzer 31. Should support monitoring unlimited number of nodes logically.	1. There could be any number of nodes in the OCAC's network, but there would be licensing on the basis of Flows Per Minute	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
155	7.5 Network Traffic Analyzer	67	35. Appliance should have hot swappable dual power supply.		The criteria is kept as per the criticality of the solution and requirement.
156	Network Traffic Analyzer	67	7.5 Network Traffic Analyzer Should support scalability in number of ports for expansion	We are presuming that OCAC would be fine with stacking of Network Behaviour and Anomaly Detection appliance or additional deployment of Network Behaviour and Anomaly Detection software installation for scalability	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
157	7.5 (33) Network Traffic Analyzer	67	Should support minimum 5,00,000 HTTP transactions.	1. This is OEM specific point, request you to remove this point. Sizing criteria for 10Gbps is already mentioned in point 29. 2. We are presuming that 500000 HTTP transactions is eqi.euivalent to 500000 Flows Per Minute i.e. the number of unique flow records per minute. Could you please let us know if this assumption is correct. 3. Clause to be reworded as "Sould support 5,00,000 HTTP transactions within 10Gbps of throughput performance"	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
158	7. Minimum technical requirement (IT assets)	67	7.5 Network Traffic Analyzer	What is the network Flows Per Minute to be considered for Network Traffic Analysis or what are the number of workstations and servers in IT network in scope?	The criteria is kept as per the criticality of the solution and requirement.
159	7. Minimum technical requirement (IT assets)	67	7.5 Network Traffic Analyzer Should be licensed to monitor traffic from unlimited number of nodes	The licensing si done on the basis of Network Flows Per Minute. If the Flow Volume Per minute is not known already then we are presuming that OCAC would provide us their IT inventory for us to determine the Flow license. Could you please confirm on this.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
160	7.5 Network Traffic Analyzer	67	40. Should be able to generate and retrieve reports within the appliance itself without the use of any additional database server.	We request that the requirement be changed accordingly	The criteria is kept as per the criticality of the solution and requirement.
161	7.5 Network Traffic Analyzer	68	41. Should be able to integrate with external storage devices for storing and retrieving if old records / data.		The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
162	7.6 Threat Intelligence feeds	68	Threat Intelligence feed OEM should have experience of at least 10 years.	As 10 year is a lesser time for the inteligance, so request you to modify the point for better intelligence "Threat Intelligence feed OEM should have experience of at least 20+ years"	The criteria is kept as per the criticality of the solution and requirement.
163	7.6 "Threat Intelligence feeds" Clause 3	68	The Threat Intelligence Portal/Dashboard should provide a complete range of adversary and technical intelligence.	This clause is a Duplicate of Clause no 2 in "Intelligence feeds". Kindly remove this clause.	The criteria is kept as per the criticality of the solution and requirement.
164	7.6 "Threat Intelligence feeds" Clause 5	68	Intelligence feeds should adhere to MITRE and ATT&CK framework.	MITRE & ATT&CK is not applicable to all the threat intel feeds or attacks. Kindly ammend this clause as below "Intelligence feeds should adhere to MITRE and ATT&CK framework wherever applicable"	The criteria is kept as per the criticality of the solution and requirement.
165	7.6 "Threat Intelligence feeds" Clause 6	68	Threat Intelligence feeds should contain who, how and why are you being targeted.	Please clarify this point as attacker motive (WHY) cannot be known always. Kindly ammend this clause as below "Threat Intelligence feeds should contain ioc, hashes,URL etc and should provide reports giving visibility into attacker motivation,adversarial methods	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
166	7.6 "Threat Intelligence feeds" Clause 7	68	Intelligence feeds should be integrated with SOAR / SIEM solution and should be pushed towards the respective devices for upgradation.	Please clarify, as Threat intel feeds providers provide API's so that others can integrate with it. Kindly ammend this clause as below "Intelligence feeds should be integrated with SOAR / SIEM solution and should provide API's to integrate."	The criteria is kept as per the criticality of the solution and requirement.
167	7.6 "Threat Intelligence feeds" Clause 9	68	The intelligence feeds should be available for the complete proposed solution and pushed periodically.	Please clarify as Kindly remove this point as intergation with SIEM/SOAR has been asked in clause 7 this clause is a duplicate.	The criteria is kept as per the criticality of the solution and requirement.
168	7.6 "Threat Intelligence feeds" Clause 10	68	Intelligence feeds from all sources should be provided as a bundled single input.	as threat intel feed is always given as output.Kindly ammend this clause as below "The threat intelligence information should include tags that help the organization to identify the indicators and threat artefacts relevant to the organization. For example, a tag might flag the fact that a file is used to target government or defence in the region"	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
169	7.6 "Threat Intelligence feeds" Clause 14	68	Should provide advanced IP Reputation.	Please Clarify "IP Reputation" Kindly ammend this clause as below so as to get more details from threat perspective and not only limited to IP address reputation only "The threat intel feed should be able to provide information (summary, related IPs, URLs, etc) of the current threat activity to be able to rapidly respond"	The criteria is kept as per the criticality of the solution and requirement.
170	7.6 "Threat Intelligence feeds" Clause 15	68	Should provide the data feed in formats interceptable by the SOC solutions	Please clarify "SOC solutions" as it's not a clear statement. Kindly remove this clause as it's a duplicate of clause 12 of Intelligence feeds.	The criteria is kept as per the criticality of the solution and requirement.
171	7.6 "Threat Intelligence feeds" Clause 17	68	Should provide additional information in IOCs wherever requested.	Please clarify "additional information" This clause can be read as below "The feeds should not only provide a series of individual data points but also correlate and analyse disparate data points and draw informed conclusions "	The criteria is kept as per the criticality of the solution and requirement.
172	7.6 "Threat Intelligence feeds" Clause 21	68	Intelligence feeds should cater to all SOC solutions and equipment.	Please clarify as it's a duplicate point to clause 7.Kindly remove this point as intergation with SIEM/SOAR from central integration perspective has been asked in clause 7 this clause is a duplicate.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
173	7.6 "Threat Intelligence feeds" Clause 22	68	Intelligence feeds should also preferably include feeds from the OEM providing the security hardware in-order to provide an integrated cyber-defense and data exchange between devices.	Please clarify this point as it conflicts to clause 19 of Intelligence Feeds which state that "Threat Intelligence feed has to be unique. This has to be from a different OEM and not the same as of SIEM / SOAR OEM to adhere to the dual incident monitoring design principle."	The criteria is kept as per the criticality of the solution and requirement.
174	7.6 Threat Intelligence feeds	68	Intelligence feeds should be available from open sources, commercial sources and international sources.	1. Is there any threat intelligence solution deployed in existing environment? Is yes, can bidder leverage same?

2. Kindly clarify the category-wise number of threat intelligence feeds required i.e. no. of open source, commercial sources and international sources. | Bidder to assess the requirement mentioned in the RFP document and propose accordingly. |
| 175 | 7.6 Threat Intelligence feeds | 68 | General | Please confirm , whether separate Threat Intelligence feeds are required or the Threat intelligence feeds available by default with various security solutions (As proposed as per RFP requirements) can be leveraged. | Bidder to assess the requirement mentioned in the RFP document and propose accordingly. |
| 176 | 7.6 Threat Intelligence feeds | 68 | General | This is only a subscription based , No product or solution needs to be proposed.

Please confirm. | Bidder to assess the requirement mentioned in the RFP document and propose accordingly. |

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
177	7.7 Network Management Switch for Data centre	69	Should have minimum 24 x 10GE SFP+ ports.	1. As per Industry standard, switches are usually comes with either 24x10G SFP+ form factor combination with higher uplink option like 40G and 100G .Switch with 40G/100G iterface availability is usefull for inter switch connectivity and higher uplink ports for future integration.Request to please change this clause as "Should have minimum 24 x 10 GE SFP+ ports and 2x40G ports and solution should be scalable to support total 48x10 SFP+ and 4x 40G QSFP+ ports without replacing the hardware".This will ensure better scalability and ROI.	The criteria is kept as per the criticality of the solution and requirement.
178	7.8 Table SI no 32 & 33	70	Minimum 4 x 1 GE Base-T interfaces Minimum 4 x 10 GE SFP+ interfaces	The throughput being asked for the router is only 20 Gbps which indicates that the bandwidth of the links which are expected to be terminated on these routers will not be 10Gbps and hence it is not needed to ask for 4 X 10 Gbps interfaces, rather we should look for more number 1G interfaces and reduce the 10Gbps interface to 2. This will enable the bidders to complete the deployment properly. Requesting to modify the clause as below: Minimum 6 x 1 GE Base-T / SFP interfaces Minimum 2 x 10 GE SFP+ interfaces	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
179	7.9 Table SL no 3	71	Should have internal redundant cooling fan.	Request to rephrase the clause as below to ensure that the whole switch does not need a replacement if the fans go faulty and it can be changed in the field without changing the entire switch: "Should have field replaceable and redundant cooling fan."	The criteria is kept as per the criticality of the solution and requirement.
180	7.1 Functionality	72	The bidder to propose relevant SAN switch for the SAN storage in redundant high availability.	Request to please change and read it as " The bidder to propose relevant SAN switch for the SAN Unified storage in redundant high availability."	Bidder to assess the deployment and propose Storage solution accordingly.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
181	7.10 Table	72	SAN Storage	Based on our understandinng of the overall SOC architecture, there are various application needed to run the SOC operations, which has also been asked for in the RFP, however,we do not see any server platform being asked for running those applications. Further, the need for a SAN switch and a SAN storage has been asked which is a little outdated from a next-gen compute and storage architecture. Currently, the widely used architecture refers to the usage of a hyperconverged node which is capable of providing compute, storage and network on a single box , that eliminates the need of components like SAN switch and a separate storage box. The scalability offered in such hyperconverged boxes are more than sufficient to offer the required amount of scalability from both compute and storage resources perspective. Hence, we strongly recommend to utilise the hyperconverged nodes here in this prestigious project.	Bidder to assess the deployment and propose Storage solution accordingly.
182	7.10 SAN Storage SI no 10	72	Should support automated SAS storage tier feature across the populated drives.		Bidder to assess the deployment and propose Storage solution accordingly.
183	7.10 Technical specification*	73	The storage system should be scalable.	Request to please change and read the clause as "The system should be scalable and support a minimum of 450 disks in a dual controller architecture and maximum of 1800 disks while scaling to 8 controllers."	Bidder to assess the deployment and propose Storage solution accordingly.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
184	7.10 point 12	73	Usable storage capacity of minimum 200 TB from Day 01 and scalable up to 1 PB.	Please revise as "Usable storage capacity of minimum 200 TB from Day 01 and scalable up to 400 TB. Offered storage should be configured for minimum 20,000 IOPS 70:30 Read:Wtite and 4K Block size". It's better to have enhanced scalability as well as minimum performance ask from day-1.	Bidder to assess the deployment and propose Storage solution accordingly.
185	7.10 SAN Storage	73	Technical Specification :- 18. Should support remote replication and replication license included.	Kindly share the source and target locations for replication with an architecture diagram and defined RTO and RPO with applicable SLA terms/timeline.	Bidder to assess the deployment and propose Storage solution accordingly.
186	7.10 SAN Storage	73	19. Synchronous and Asynchronous replication support should be available with relevant licenses.	Please provide the distance between source and target locations to decide the type of replication.	Bidder to assess the deployment and propose Storage solution accordingly.
187	7.11	73	Vulnerability assessment solution	Please clarify how many IPs are in scope for VA and what would be the frequency of assessment.	The criteria is kept as per the criticality of the solution and requirement.
188	7.11 Vulnerability Management Solution-Funtionality	73	Bidder to propose and implement virtual machine for deployment of Vulnerability Management Solution	Please clarify who will provide the resource for the deploymnet	The criteria is kept as per the criticality of the solution and requirement.
189	7.11 Vulnerability Management Solution-Funtionality	73	Vulnerability management solution should be based on 512 floating IP addresses (IPs can be changed and active scanning can be done as per requirement) from Day 01 and can be increased as per requirement.	Please clarify is that 512 Qty is treated as Qty-1 in the BOQ . And if any increase in the IP or requirmnet , then OCAC will procure another set of 512 Qty .	The criteria is kept as per the criticality of the solution and requirement.
190	7.11 Vulnerability Management Solution	73	General	Please provide approximate count of IP Addresses/Device details which needs to be scanned through Vulnerability Management solution.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
191	7.12 Network Monitoring, Helpdesk and Ticketing tool	74	The network monitoring tool must monitor performance across heterogeneous networks from one end of the enterprise to the other.	NMS/EMS consists of multiple components. Having all these components from the same OEM will ensure that the components are pre-integrated and adequately tested and hence time to value realization is quick and issues of integration does not arise. Hence requesting you to please update the specification as follows: "The network monitoring tool should be an integrated, modular and scalable solution from single OEM to monitor performance across heterogeneous networks from one end of the enterprise to the other. (i.e. all Network Monitoring, server and database monitoring and Service Management tools should be from single OEM) to provide comprehensive fault management, performance management, traffic analysis and business service management, IT service desk\ help desk \trouble ticketing system & SLA monitoring functionality."	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
192	7.12 Network Monitoring, Helpdesk and Ticketing tool	75	Proposed NMS solution must be ISO 27001 certified to ensure security compliances.	ISO 27034-1 standard helps organizations integrate security controls in the software through their software development cycle, by defining security frameworks & vulnerability management processes. This certification protects customer assets from potential cyber breaches & security threats while complying with the Application security standards. It addresses all aspects from determining information security requirements, to protecting information accessed by an application as well as preventing unauthorized use and/or actions of an application. Hence requesting you to please update the specification as follows: "Proposed NMS solution must be ISO 27001 and ISO 27034 certified from a verification or certification agency which has global recognition to ensure security compliances." Would request you to remove the	The criteria is kept as per the criticality of the solution and requirement.
193	7.12 Network Monitoring, Helpdesk and Ticketing tool	74		As per the BOM Network Monitoring, Helpdesk & Ticketing software Qty is - 1 , As all the License is calculated based on the Nos of device for NMS and nos of Cuncurrent user for the Helpdesk - requesting please share the nos of devive and Helpdesk Agent	The criteria is kept as per the criticality of the solution and requirement.
194	7.12 Network Monitoring, Helpdesk and Ticketing tool	74		Please clarify who will provide the resource and storage for the deploymnet	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
195	7.12 Network Monitoring, Helpdesk and Ticketing tool	74	4. Proposed NMS solution MUST have at least 2 deployments in Indian Government/ Public Sector, monitoring & managing 2500+ network nodes in each of such deployments. Customer names, solution details and OEM undertaking needs to be provided at the time of bidding.	Please remove the clause since these are confidential information and cannot be shared. Existing clause favors a particular OEM who has existing tools deployment in this state Govt.	The criteria is kept as per the criticality of the solution and requirement.
196	7.12 Network Monitoring, Helpdesk and Ticketing tool	75	OGC Gold level or Pink Elephant certifications for ITILv3 in at least 10+ processes or equivalent.	Please change it to Pink Elephanr certifications for ITIL v4 for 5 practices since ITIL v3 is earlier version and has less relevance now.	The criteria is kept as per the criticality of the solution and requirement.
197	7.12 Network Monitoring, Helpdesk and Ticketing tool	74	6. The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.	"The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date."	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
198	Section 7, Sub-Section 7.12, Clause 8.	75	The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e. Router, Switches, Servers, etc.) and map the connectivity between them with granular visibility up to individual ports level.	Please confirm that the scope of devices envisaged to be monitored by NMS is confined to the assets mentioned under Annexure 1 and the IT assets under Proforma 16. Please confirm the number of virtual servers that are envisaged to be monitored. Please confirm if Operating System & Database Monitoring and Administration is envisaged under the scope of NMS. Please list the Databases in use, and also please mention the number of Application OS and DB OS instances to be monitored. Please confirm if Application Performance Management is envisaged under the scope of NMS? If yes, please mention the number of critical applications to be monitored? Please confirm if Storage Monitoring	The criteria is kept as per the criticality of the solution and requirement.
199	Section 7, Sub-Section 7.12, Clause 18.	75	The system should be able to clearly identify configuration changes / policy violations / inventory changes across multi-vendor network	Please confirm if Patching, Provisioning, Configuration for Servers and Desktops is envisaged under the scope of NMS?	The criteria is kept as per the criticality of the solution and requirement.
200	7.12 Network Monitoring, Helpdesk and Ticketing tool	76	The solution should be able to integrate with SOAR solution.	There should be a tight bi-directional integration between NOC, SOC and SOAR to have the single consolidated console of Infrastructure & security events and automated actions.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
201	7.12 Network Monitoring, Helpdesk and Ticketing tool	75	34. Should use Industry-standard protocols such as WMI, SNMP, JMX, SSH to perform discovery without requiring the installation of an Agent.	This point is favoring a particular OEM and jmx discovery is outdated and there are many new ways to do weblogic discovery. Please change this point to "Should use Industry-standard protocols such as WMI, SNMP, SSH etc. to perform discovery without requiring the installation of an Agent."	The criteria is kept as per the criticality of the solution and requirement.
202	7.12 Network Monitoring, Helpdesk and Ticketing tool	75	36. Discovery should work without requiring agent installation (that is, agent-less discovery) while discovery Layers 2 through Layers 7 of OSI model	Please modify it as "Discovery and application dependency mapping should work without requiring agent installation (that is, agent-less discovery) while discovery Layers 2 through Layers 7 of OSI model	The criteria is kept as per the criticality of the solution and requirement.
203	Section 7, Sub-Section 7.12, Clause 38.	76	The solution should have internal storage and function without any third party database.	This point is favoring a particular OEM. Please remove this point.	The criteria is kept as per the criticality of the solution and requirement.
204	Section 7, Sub-Section 7.12, Clause 43.	77	The solution should support at least 2 administrator user accounts and at least 10 user accounts.	Please provide the total nos. of Helpdesk (HD, Change, KM, SLM etc.) agents logging into the helpdesk system?	The criteria is kept as per the criticality of the solution and requirement.
205	7.13 Desktop Sr 34	78	Desktop should have power consumption of 180W with 90-95% efficiency		The criteria is kept as per the criticality of the solution and requirement.
206	8. Manpower for CSOC	79	8.1 Manpower Requirement	We request you to kindly consider Non IT Manpower (Electrical / HVAC Engineer) to be included to manage the IBMS, Electrical and HVAC Systems of the Entire CSOC for the day to day Maintenance.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
207	8.2 Manpower qualification L1 Analyst	80	• B.E / B-Tech / MCA / Diploma in relevant field. • Minimum of 3 years of experience in security device administration & management. • Have experience in vendor management, patch management, Helpdesk and incident management. • Certified in ITIL v3 or later version. • ISO 27001:2013 or later version certification preferred.	ITIL certificate for an operational resource with 3 years of experience is not a valid selection criteria. Product experience with OEM certificate and day to day activities on the product will be valid criteria for tenderer to select. Requesting to please remove Certification in ITIL v3 or later version/ISO 27001(any one) preferred We request OCAC to kindly amend the clause as below: • B.E / B-Tech /MCA • Minimum of 3 years of experience in SOC/NOC services through on-premises or managed mode of service provider. • Minimum 2-year experience in operating a SIEM product and other security tools. • Have experience in handling log management and incident management. • CEH/ECSA or equivalent certified	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
208	8.2 Manpower qualification	80	• B.E / B-Tech with MBA • Minimum 10 years of experience out of which, minimum 6 years relevant experience in management from reputed organizations. • Must have experience of 2 to 3 years with a cybersecurity domain project and associated with a cybersecurity organization. • Certification in PMP, PRINCE2, CPMP, PgMP, CSM etc. (any one).	Kindly modify as follows:- • B.E / B-Tech ~~with~~ / MBA • Minimum 10 years of experience out of which, minimum 6 years relevant experience in management from reputed organizations. • Must have experience of 2 to 3 years with a cybersecurity domain project and associated with a cybersecurity organization. • Certification in PMP, PRINCE2, CPMP, PgMP, CSM etc. (any one). May we request you to kindly modify the clause as below: • B.E / B-Tech/M. Tech/MCA/MBA • Minimum 10 years of experience out of which, minimum 6 years relevant experience in management from reputed organizations. • Must have experience of 2 to 3 years with a cybersecurity domain project and associated with a cybersecurity organization. • Certification in PMP, PRINCE2, CPMP, PMP, CISM, CISA, CISSP	The criteria is kept as per the criticality of the solution and requirement.
209	8.4 Additional Manpower requirement	84	In the BOQ section Cost estimate for proposed Manpower	Please clarify the Unit cost will be Per Year for each type of additional Manpower and how Bidder will Bill to OCAC and what is the calcullation method	All billing to be done as Quarterly Guaranteed Revenue (QGR)

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
210	8.4 Additional Manpower	84	Threat Hunting Specialist: Qualification required: • Minimum 10 years of experience in Security Operations Centre (SOC) or Cyber security domain. • Have knowledge about all the solutions implemented in SOC. • Have minimum 3 years of experience as a red team or blue team member. • Must have scripting knowledge and not totally depend on automated solutions.	May we request you to kindly modify the clause as: • Minimum 6 years of experience in Security Operations Centre (SOC) or Cyber security domain. • Have knowledge about all the solutions implemented in SOC. • Have minimum 2 years of experience as a red team or blue team member. • Must have scripting knowledge and not totally depend on automated solutions.	The criteria is kept as per the criticality of the solution and requirement.
211	8.4 Additional Manpower	84	Security Trainer: Qualification required: • Minimum 10 years of experience with any security solution OEM. • Have relevant knowledge with security solution at different level of security architecture. • Have hands on experience with security solution interface and configurations. • Have experience in providing security related training and conferences to enterprises for cyber risk related matter • and technology.	May we request you to kindly modify the clause as: • Minimum 6 years of experience with any security solution OEM. • Have relevant knowledge with security solution at different level of security architecture. • Have hands on experience with security solution interface and configurations. • Have experience in providing security related training and conferences to enterprises for cyber risk related matter and technology.	The criteria is kept as per the criticality of the solution and requirement.
212	9.1.1 Device and software availability	88	The uptime of SOC devices (example: switch, Anti-APT, SAN switch, SAN, Log appliance, etc.) should be taken as a whole and the SLA would be calculated as the average of the device's uptime.	We request OCAC to relax the uptime for specific devices as some of the devices like Anti-APT would not be able to meet >=99.90 % uptime target.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
213	9.1.2 Incident logging and Response	89	Timeline for isolation of the threat or vulnerability through CSOC operations / bypass of the system – the next 30 minutes.	Request you to change the clause as Timeline for isolation of the threat or vulnerability through CSOC operations / bypass of the system – the next 60 Minutes Critical---> High We request OCAC to kindly clarify on this statement and revise this, as the mitigation timeline will depend on attack type and not feasible be fixed within 3 hours.	The criteria is kept as per the criticality of the solution and requirement.
214	9.1.2 Incidense Response Table	89	SLA for Critical: Mitigation of incident - Less than the next 3 hours SLA for High: Mitigation of incident - Less than the next 6 hours	We request OCAC to increase the mitigation timeline of the incident, else revise the clause basis the incident occurred and its type & intensity.	The criteria is kept as per the criticality of the solution and requirement.
215	9.1.2	89	Scenario 1: When the bidder has full control and authority for the mitigation of the incident	Can you please share an example when the bidder has full control od the mitigation of the incident?	The criteria is kept as per the criticality of the solution and requirement.
216	9.1.3	91	100% Attendance	100% attendance is not possible in case where only one resource is deployed in that category Example CSOC Manager. Request to relax to a reasonable limit.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
217	9.1.5, Business Continuity Plan testing, Sl. No.1	92	Target: A BCP drill should be conducted once every year (with minimum gap of six months from previous BCP drill) to test the redundancy and point of failures in the SOC design.	As per our understanding BCP drill must be conducted once in a year i.e. on or before completion of the year. Please confirm. Part of BCP testing, there is expectation of annual drill for devices in high availability, network as redundancy and services as redundancy. Are you expecting all the CSOC devices in HA mode? Are you also expecting to provision redundancy in your DR center, in case main CSOC devices hosted in DC are unavailable? In section 13. Bill of Materials for CSOC the quantity for SIEM / SOAR / VM / NTA etc is 1 and for APT is 2 Part of BCP testing, there is expectation of annual drill for devices in high availability, network as redundancy and services as redundancy. Part of Services redundancy, are you expecting alternate location identified for serving the CSOC in case the main	The criteria is kept as per the criticality of the solution and requirement.
218	9.1.9 Civil & Electrical Works	93	Target SLA: 100% Operational 24*7*365	Civil Works are generally covered by defect liability period which lasts for 12 months in all giovernment contracts. Depending on the usage, there will be wear & tears which are not covered beyond DLP. Moreover people will use the Chairs / Console etc. for their Day to Day work and hence there cannot be any SLA on the same. So we request you to kindly remove the SLA for Civil Works	The criteria is kept as per the criticality of the solution and requirement.

Sl #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
219	9.1.9 Civil & Electrical Works	93	General Point : There is no Diesel Generator (DG) requirement in the Scope	Please clarify if DG is already availaible at site to cater to the Power Requirement of entire SOC in case Grid Power fails. If yes we need the following details also: a) Rating of DG b) Redundancy Scheme.	The criteria is kept as per the criticality of the solution and requirement.
220	10. Project Timelines	94		Considering the importance and complexity in setting the things up in right manner 8 months from MSA Signing looks good, request you to look in to the same and change the timelines.	The criteria is kept as per the criticality of the solution and requirement.
221	10. Project Timelines	94	5. Supply, Installation and Commissioning of all IT Equipment	Considering the importance and complexity in setting the things up in right manner 8 months from MSA Signing looks good, request you to look in to the same and change the timelines. We request you to kindly clarify on below: Does the 6 weeks (T0 + 22 Weeks) include integration of all IT assets of OSDC, OSWAN and Odisha State IT Centre to SIEM solution, if so request to increase the timelines to at least 24 weeks (T0 + 40 weeks).	The criteria is kept as per the criticality of the solution and requirement.
222	11 Payment Terms	96	Entire Clause	We request OCAC to consider 10% advance payment for the CAPEX part, which is a standard practice in such kind of projects.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
223	11	96	11. Payment terms (For serial no 1,2,3)	Request to please amend the payment clause from 80% to 90%, considering high amount of CAPEX involved in the project. Please associate respective percentage to each state. Initial investment would be very high. Kindly Amend with Brekup Payment Term::20% on Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval;Payment 30% Finalization and Approval of the submitted layout, Floor diagram, Non-IT and IT architecture, etc.;Payment 30% Completion of Structural, Architectural, Civil & Interior Works	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
224	11. Payment terms; Sr No: 1,2&3	96	1. Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval 2. Finalization and Approval of the submitted layout, Floor diagram, Non-IT and IT architecture, etc. 3. Completion of Structural, Architectural, Civil & Interior Works. Payment Terms: 80% of the quoted cost for the activity (civil and interior works)	1. Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval 2. Finalization and Approval of the submitted layout, Floor diagram, Non-IT and IT architecture, etc. Payment Terms: 40% of the quoted cost for the activity (civil and interior works) 3. Completion of Structural, Architectural, Civil & Interior Works. Payment Terms: 40% of the quoted cost for the activity (civil and interior works)	The criteria is kept as per the criticality of the solution and requirement.
225	11	96	Payment terms regarding manpower of CSOC	Request to please amend the terms as "Quarterly in advance".	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
226	11	96	All payments would be done after evaluation and approval of the Payment Approval Committee (PAC) constituted by OCAC within 30 days from the date of submission of invoice. Any dispute / discrepancy around the invoice needs to be raised within 20 days of the invoice submission	All payments would be done after evaluation and approval of the Payment Approval Committee (PAC) constituted by OCAC within 30 days from the "date of invoice" instead of "date of submission". Kindly amend the below clause as: All invoices and bills will be raised by Bidder as per the Payment Terms and will become due for payment within thirty (30) days of presentation. All payments due for more than thirty (30) days will attract an interest at the rate of 2 percent per month on the invoice amount calculated from the date the payment became due until the recovery is made in full with interest. Without prejudice to the other rights available, Bidder also reserves the right to withhold the provision of services till such time all the payments due to it under this Agreement have been made by BUYER and any such withholding by the Bidder shall not be treated as breach by it of the provisions of this	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
227	11	96	Payment terms	The bidder requests the following modifications: 1. Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval - 20% of the quoted cost for the activity (civil and interior works) 2. Finalization and Approval of the submitted layout, Floor diagram, Non-IT and IT architecture, etc. - 20% of the quoted cost for the activity (civil and interior works) 3. Completion of Structural, Architectural, Civil & Interior Works - 50% of the quoted cost for the activity (civil and interior works) 4. Supply of all Non-IT asset. (excluding the civil and interior works) - 60% of quoted cost by the bidder for Non- IT items (excluding the civil and interior works) 5. Installation and Commissioning & Testing of all Non-IT asset. (excluding the civil and interior works) - 30% of quoted cost by the bidder for Non- IT items (excluding the civil and	The criteria is kept as per the criticality of the solution and requirement.
228	11. Payment terms	98	For the first year period, any payment towards operations and maintenance would not be made to the bidder, although any penalty towards breach of SLA for the period would be applicable to the bidder.	We understand that Bidder has already submitted 10% of PBG in case of any breach same can be encashed. But Since Bidder shall be incurring cost in first year of O&M as well. We request you to kindly pay Bidder in first year as well. We request OCAC to revise or remove this clause & clarify if this is for AMC.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
229	11. Payment terms	98	Operations and maintenance cost (for IT and Non-IT items) - 36 months (no payment towards O&M would be made to the successful bidder during the first year of O&M phase) Quarterly O&M payment = OPEX cost / 12	We request you to kindly modify as follows:- Operations and maintenance cost - 36 48 months (no payment towards O&M would be made to the successful bidder during the first year of O&M phase) Quarterly O&M payment = OPEX cost / 12 16 Please clarify this point please , is that 1 st yeasr O&M cost including Manpower will be part of the Opex . Kindly Amend The Operations and Maintenance schedule to Yearly advance against submission of IT OEM backlining aggrement for the year The bidder requests the following modifications: Operations and maintenance cost - 48 months (Quarterly O&M payment = OPEX cost / 16)	The criteria is kept as per the criticality of the solution and requirement.
230	11.1 Penalty 11.1.1 Supply, Installation, Commissioning	99	Milestone Penalty	We request you to kindly remove milestone Penalty. Please Modify as Deduction of 0.5% per week of uncompleted portion post Sign-off & FAT- after 24 weeks. Subject to maximum of 20% of the CAPEX.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
231	11.1.1	99	11.1.1 Supply, Installation, Commissioning Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval Finalization and Approval of the submitted layout, etc. Completion of Structural, Architectural, Civil & Interior Works.	Request to amend it to 0.5% of the prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment.	The criteria is kept as per the criticality of the solution and requirement.
232	11.1 Penalty 11.1.1 Supply, Installation, Commissioning	99	Milestone Penalty SI. 1-3 Deduction of 1% of the prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment. SI. 4. Deduction of 2% of the prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment. SI. 5. Deduction of 2% of the prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment.	We request you to kindly modify as follows:- Milestone Penalty SI. 1-3 Deduction of 1% of the Undelivered portion of prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment. SI. 4. Deduction of ~~2%~~ 1% of the Undelivered portion of prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment. SI. 5. Deduction of ~~2%~~ 1% of the Undelivered portion of prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment. SI no. 1,2 & 3 We request you to kindly amend the clause as below: Timeline suggested = T0+6 weeks , T0+8 weeks and T0+18 weeks, and Then penalty will be 0.5% and	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
233	11.1 Penalty 11.1.1 Supply, Installation, Commissioning	99	Finalization and Approval of the submitted layout, etc.	We understand time taken for approval and modification given by Customer shall be excluded while calculating Penalty. Please confirm. Kindly confirm all the approvals shall be given within 7-14 days post submission of documents.	The criteria is kept as per the criticality of the solution and requirement.
234	11.1	99	Supply, Installation and Commissioning & Testing of all Non-IT asset. Supply, Installation and Commissioning of all IT Equipment	Request to amend it to 0.5% of the prescribed payment for the milestone for every week of delay subject to maximum of 20% of the prescribed payment.	The criteria is kept as per the criticality of the solution and requirement.
235	11.1.1 Supply, Installation, Commissioning	99	All penalties related to supply, installation and commissioning is capped at 20% of the prescribed payment for the respective milestone	Kindly amend the below clause as: All penalties related to supply, installation and commissioning is capped at ~~20%~~ 5% of the prescribed payment for the respective milestone	The criteria is kept as per the criticality of the solution and requirement.
236	11.1	100	Project Sign-Off & FAT (Go-Live of the Project)	Request to amend it to 0.5% of the prescribed payment for the milestone for every week of delay subject to maximum of 10% of the prescribed payment.	The criteria is kept as per the criticality of the solution and requirement.
237	11.1.1	100	Supply, Installation, Commissioning Penalty clause for Sr. 5	The bidder requests the following modifications: Sr. 5 - Deduction of 1% of the prescribed payment for the milestone for every week of delay subject to maximum of 5% of the prescribed payment.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
238	11.1 Penalty 11.1.1 Supply, Installation, Commissioning	100	Deployment of manpower proposed for SOC-Within 15 days of successful PAT / UAT of the SOC infrastructure.	We will try our best to onboard and deploy manpower as soon as possible but it mostly depends on Manpower Location ,Shifting time required ,Medical conditions etc. Hence Kindly modify as below :- Deployment of manpower proposed for SOC-Within 15 45 days of successful PAT / UAT of the SOC infrastructure. The bidder requests the following modifications: Within 30 working days of successful PAT / UAT of the SOC infrastructure.	The criteria is kept as per the criticality of the solution and requirement.
239	10.1.1 , Table point no 7	100	15 Days: 10,000 per individual manpower	Requested for 20 Days, Rs 3000 per individual manpower The bidder requests the following modifications: Rs. 10,000/- per individual manpower / per week of delay to be capped at 100% of the monthly manpower rate quoted. To be measured on pro-rata basis as per deployment of manpower.	The criteria is kept as per the criticality of the solution and requirement.
240	11.1.2 Operations and Maintenance	100	Overall SLA penalty amount related to operations and maintenance is capped at a maximum value of 20% of the QGR amount.	Overall SLA penalty amount related to operations and maintenance is capped at a maximum value of 2010% of the QGR amount. Request to reduce the cap to 10% of QGR amount.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
241	11.1.2 Operations and Maintenance	100	Penalty for Incident logging : Rs. 5000 for every incident not logged	Request you modify the penalty amount as below which is reasonable Penalty for Incident logging : Rs. 5,000 1,000 for every incident not logged	The criteria is kept as per the criticality of the solution and requirement.
242	11.1.2 Operations and Maintenance	100	Overall SLA penalty amount related to operations and maintenance is capped at a maximum value of 20% of the QGR amount.	As a standard practice in similar government contracts, we request OCAC to cap the penalty at 10% of the QGR amount.	The criteria is kept as per the criticality of the solution and requirement.
243	11.1.2, Incident Management	101	100% logging of all alerts and security incidents. 100% logging of all department / official reporting of incidents	We request OCAC to reconsider the penalty terms for this clause as logging depends on the ticketing tool & timelines along with the Events getting logged basis EPS.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
244	11.1.2 Operations and Maintenance	103	Penalty for Device uptime / Device availability: >=99.90%: No penalty >=98.00%; <99.90% 0.5% of QGR value >=95.00%; < 98.00% 1% of QGR value <95.00% 1% of QGR value for very percentage drop	Request you modify the penalty amount as below which is reasonable >=~~99.90%~~ 99.00%: No penalty >=98.00%; <99.90% ~~0.5%~~ 0.1% of QGR value >=95.00%; < 98.00% ~~1%~~ 0.5%of QGR value <95.00% ~~1%~~ 0.5% of QGR value for very percentage drop Please clarify expectation. Do you need past data to be made available within the stipulated time or, restoration of system/service availability is the only expectation? Kindly amend the below clause as: Uptime-99.90% The time lost due to any of the following reasons shall be taken into account while calculating the availability/ uptime requirement: (a) Time lost due to power or environmental failures; (b) Time taken to recover the system because of power or environmental failures; (c) Time lost due to damage or malfunction in the system or any	The criteria is kept as per the criticality of the solution and requirement.
245	11.1.2 Operations and Maintenance	103	Penalty for SOC application / software availability: >=99.90%: No penalty >=98.00%; <99.90% 0.5% of QGR value >=95.00%; < 98.00% 1% of QGR value <95.00% 1% of QGR value for very percentage drop	Request you modify the penalty amount as below which is reasonable >=~~99.90%~~ 99.00%: No penalty >=98.00%; <99.90% ~~0.5%~~ 0.1% of QGR value >=95.00%; < 98.00% ~~1%~~ 0.5%of QGR value <95.00% ~~1%~~ 0.5% of QGR value for very percentage drop	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
246	11.1.2, Operations and Maintenance, Service Availability, Sl. No. 3	104	Penalty Terms	As we all know landscape of technology is changing day by day, therefore, in order to enhance knowledge, we encourage our resources to learn new technology/solutions. We request to grant approval of 5 days for training in year for each resource (excluding the holidays mentioned in RFP). Also, we request you to modify the penalty clause as below: Level 1 resource absent (without approval): Equal cost of the resource proposed by the bidder per day on pro rata basis. CSOC engineer and Level 2 resource absent (without approval): Double the cost proposed by the bidder per day on pro rata basis. Security Admin and Threat Intel expert and SOC Manager absent	The criteria is kept as per the criticality of the solution and requirement.
247	12. Reporting, 7. Vulnerability assessment report*	107	Quarterly basis / On real time / request basis - List of vulnerabilities observed in the system. - List of risks and vulnerabilities observed in the application. - Action taken against each vulnerability. - Risk details of each vulnerability. - Recommendation against each vulnerability.	We request OCAC to put a cap on the number of applications and devices for assessment in a quarter.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
248	13. Bill of Materials for CSOC	109	*Log Management appliances should be proposed as 4 nos. in quantity if existing asset is to be upgraded and utilized and 6 nos. quantity to be proposed if new assets and solutions are to be proposed by the bidder.	Kindly provide the Existing SIEM EOL? Requesting to clarify regarding the qty (4/6) Different OEM has different solution criteria, the quantity needs to be decided by OEM to meet the technical specifications and scope Request you to not put a hardnumber to quantity for scenario where overall new SIEM is proposed by bidder Please clarify whether OCAC wants to deploy the Logger with Connector in high availavbility mode for all 3 locations? Different OEM has different solution criteria, the quantity needs to be decided by OEM to meet the technical specifications and scope Request you to not put a hardnumber to quantity for scenario where overall new SIEM is proposed by bidder Different OEM has different solution	The bidder to deploy the log management appliance in pairs as redundant and high availability at OSDC, OSWAN and State IT centre.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
249	13. Bill of Materials for CSOC	109	Network Traffic analyzer 1	As per the Technical Specfication ,High availablity to be considered for Network traffic analyser .But as per the Bill of material Qty 1 Nos is given . Kindly Change the Qty to 2 Nos

Though OCAC will be serving for 3 locations but the NTA solution will be placed in a single location and in standalone mode? To maintain the SLA it should be in HA (Active-Cold Standby) mode. | Proposed NTA solution shall be placed at a centralized location. |
250	13. Bill of Materials for CSOC	109	Anti – Advanced Persistent Threat Intelligence	Though OCAC will be serving for 3 locations but the Anti-APT solution will be placed in a single location and in high availability mode?	Bidder should deploy 1 no. solution at OSDC and 1 no. solution at State IT centre.
251	13. Bill of Materials for CSOC	109	Security Orchestration, Automation and Response (SOAR)	Though OCAC will be serving for 3 locations but the SOAR solution will be placed in a single location and in standalone mode?	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
252	13. Bill of Materials for CSOC	109	Security Information and Event Management (SIEM)#	Though OCAC will be serving for 3 locations but the SIEM solution will be placed in a single location and in standalone mode?	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
253	13. Bill of Materials for CSOC	109	Vulnerability Management Solution	Though OCAC will be serving for 3 locations but the VAS solution will be placed in a single location and in standalone mode? Please confirm that the bidder needs to quote 512 Ips from day one?	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
254	13. Bill of Materials for CSOC	109	Network Monitoring, Helpdesk & Ticketing software	Though OCAC will be serving for 3 locations but the ITSM solution will be placed in a single location and in standalone mode?	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
255	13. Bill of Materials for CSOC	109	Threat Intelligence feeds and updates	Though OCAC will be serving for 3 locations but the TIF solution will be placed in a single location and in standalone mode?	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
256	13. Bill of Materials for CSOC	110	Pin up Notice board	Size & Design not mentioned	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
257	13. Bill of Materials for CSOC	110	Perforated cable tray (factory made galvanized)	Qty. & size details not specified.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
258	13. Bill of Materials for CSOC	110	Cable raceway for cabling and wiring	Qty. & size details not specified.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
259	14.1	112	The proposed manpower should be deployed at SOC within 15 days of successful PAT / UAT of the complete infrastructure.	May we request to amend the clause as "The proposed manpower should be deployed at SOC within 30 days of successful PAT / UAT of the complete infrastructure."	The criteria is kept as per the criticality of the solution and requirement.
260	14.1 SI no 3	112	The certifications of the manpower resources proposed for the project should be valid during the bid submission and also for the entire duration of the project. Bidder should ensure to reissue any expired certification from the relevant body.	Considering the relevant certifications & their validity to be consistent, may we request you to please relax the clause for the certifications as below: The certifications of the manpower resources proposed for the project should be valid during the bid submission.	The criteria is kept as per the criticality of the solution and requirement.
261	14. General conditions of contract for bidder 14.1 General terms	112	All cost / price of the items quoted by the bidder would be fixed for the period of the contract and any new procurement or upgradation of the respective item would be done basis the quoted price	Since the equipment & quantities mentioned in the price schedule & layout for site preparation are indicative, we request you to confirm that the quantity can vary up to a maximum of +/- 10%.	The criteria is kept as per the criticality of the solution and requirement.
262	14. General conditions of contract for bidder 14.1 General terms	112	The successful bidder should submit the Performance Bank Guarantee to OCAC within 30 days of Letter of intent / Award of project contract.	Request you to mention the PBG percentage out of Total contract Value	The criteria is kept as per the criticality of the solution and requirement. It is 10% of Contract value

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
263	14.2	113	Insurance	EY maintains professional indemnity insurance only. Such professional indemnity insurance covers our professional liability up to an appropriate level sufficient for the purposes of this engagement. Since EY PII policy is confidential, the terms of the policy shall not be disclosed The bidder requests the following modifications: 1. Appropriate insurance to cover all solution components for the transit period and until the time of delivery at the respective site is to be taken by the successful bidder. The bidder shall bear the risk of loss on Assets up to the time they are transferred and handed over to the Purchaser - after which it shall stand transferred to the Purchaser. SI shall arrange and pay for insurance to cover such item until it is transferred and thereafter cost of insurance is to be borne by Purchaser and the Risk of Loss lies with Purchaser.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
264	14.3 Confidentiality	113	Confidentiality	We request to revise & add the below to the existing clause "Except as otherwise permitted by this Agreement, neither of the parties may disclose to third parties the contents of this Agreement or any information provided by or on behalf of the other that ought reasonably to be treated as confidential and/or proprietary. Parties may, however, disclose such confidential information to the extent that it: (a) is or becomes public other than through a breach of this Agreement, (b) is subsequently received by the receiving party from a third party who, to the receiving party's knowledge, owes no obligation of confidentiality to the disclosing party with respect to that information, (c) was known to the receiving party at the time of disclosure or is thereafter created independently, (d) is disclosed as necessary to enforce the receiving party's rights under this Agreement, or (e) must be disclosed under applicable law, legal process or	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
265	14.4	114	Indemnification: The implementation agency hereby indemnifies, hold harmless & undertakes to defend OCAC, its affiliates and their respective employees, officers and directors against any claim by a third party including but not limited to damages, costs, expenses as a result of such claim with regard to: •taxes/charges/cess/levies (and interest or penalties assessed thereon) against OCAC that are obligations of bidder pursuant to the agreement; •In event of any theft, loss, damage, destruction, or any other act of vandalism or sabotage of the property of the purchaser in the possession of the bidder by virtue of the agreement, the implementation agency shall be liable to indemnify the first part to the extent of damage or loss so caused.	We propose : The implementation agency hereby indemnifies, hold harmless & undertakes to defend OCAC, its affiliates and their respective employees, officers and directors against claims including but not limited to damages, costs, expenses as a result of such claim with regard to: OCAC notifies the implementation agency in writing in a reasonable time frame on being aware of such claim. OCAC provides the Bidder with the assistance, information and authority reasonably necessary to perform the above, and OCAC does not make any statement or comments or representations about the claim without prior written consent of the Bidder, except under due process of law or order of the court. Kindly amend the below clause as: The implementation agency hereby indemnifies, hold harmless &	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
266	14.5.1	115	Limitation of liability for implementation agency The implementation agency shall be liable to the client / purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs or loss of reputation	Kindly Amend:"Neither party shall be liable to each other, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs or loss of reputation. The bidder requests the following modifications: i) The aggregate liability of bidder (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed the total amount, paid to bidder by the Purchaser in the preceding twelve months under this Agreement that gives rise to such liability (as of the date the liability arose). ii) In no event shall bidder be liable for any consequential, incidental	The criteria is kept as per the criticality of the solution and requirement.
267	14.5 Limitation of liability for implementation agency	115	The mentioned points 14.3.1 and 14.3.2 are applicable provided they do not exclude or limit any liabilities of either party in ways not permitted by applicable law.	Request to delete this clause	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
268	14.5 Limitation of liability for implementation agency	115	14.5.2 The aggregate liability of the implementation agency to the client / purchaser, whether under the contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the successful bidder to indemnify the client with respect to intellectual property rights infringement.	Kindly modify as follows:- 14.5.2 The aggregate liability of the implementation agency to the client / purchaser, whether under the contract, in tort or otherwise, shall not exceed the 50% of the total Contract Price, provided that this limitation shall not apply to any obligation of the successful bidder to indemnify the client with respect to intellectual property rights infringement.	The criteria is kept as per the criticality of the solution and requirement.
269	14.7	116	Force Majeure	We request OCAC to add below clause to under Force Majeure to facilitate remote working : (ii) To the extent that the provision of the Services is impacted by a pandemic (including COVID-19) and any reasonable concerns or measures taken to protect the health and safety interests of either Party's personnel, the Parties will work together to amend the Agreement to provide for the Services to be delivered in an appropriate manner, including any resulting modifications with respect to the timelines, location, or manner of the delivery of Services. (iii) Where the bidder Personnel are required to be present at Client's premises, The bidder will use reasonable efforts to provide the Services on-site at [Client] offices, provided that, in light of a pandemic the parties agree to cooperate to allow for remote working and/or an extended timeframe to the extent (i) any government or similar entity implements restrictions that may	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
270	14.8	116	Intellectual Property Rights	We request to revise & add the below to the existing clause: The bidder may use data, software, designs, utilities, tools, models, systems and other methodologies and know-how ("Materials") that the bidder own in performing the Services. Notwithstanding the delivery of any Reports, the bidder retain all intellectual property rights in the Materials (including any improvements or knowledge developed while performing the Services), and in any working papers that bidder compile and retain in connection with the Services (but not Client Information reflected in them).Upon payment for the Services, Client may use any Materials included in the Reports, as well as the Reports themselves as permitted by this Agreement. <u>Kindly amend the below clause as:</u> a. In order to perform the services, Successful Bidder must obtain at its	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
271	14.9	118	Change control Implementation agency shall not charge for any cost incurred for configuration / reconfiguration of the equipment / services as directed by OCAC on account of regulatory compliance / guidelines issued by GoO and GoI.	The bidder requests the following modifications: Bidder requests to be compensated for the efforts required for configuration / reconfiguration of the equipment / services as directed by OCAC on account of regulatory compliance / guidelines issued by GoO and GoI. These can be mutually discussed and agreed and can be taken up as a Change request.	The criteria is kept as per the criticality of the solution and requirement.
272	14.10 Publicity	118	Any publicity by the implementation agency in which the name of OCAC is to be used, should be done only with the explicit written permission from OCAC.	We propose: The client, without prejudice to any other rights or remedies it may possess, may terminate the agreement forthwith in the following circumstances by giving a notice of 30 days (post 30 days notice to cure the default) for termination and its reasons therefore to the implementation agency	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
273	14.11.1	119	Termination for implementation agency's default The client, without prejudice to any other rights or remedies it may possess, may terminate the agreement forthwith in the following circumstances by giving a notice of 30 days for termination and its reasons therefore to the implementation agency:	Kindly amend the below clause as: 14.11.2.1 The client, without prejudice to any other rights or remedies it may possess, may terminate the agreement forthwith in the following circumstances by giving a written notice of 30 days for termination and its reasons therefore to the implementation agency: a. If the implementation agency becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the implementation agency is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the implementation agency takes or suffers any other analogous action in consequence of debt; b. If the implementation agency assigns or transfers the contract or any right or interest therein in violation of the	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
274	14.11.2 Termination for implementation agency's default	119	14.11.2.1 The client, without prejudice to any other rights or remedies it may possess, may terminate the agreement forthwith in the following circumstances by giving a notice of 30 days for termination and its reasons therefore to the implementation agency: a. If the implementation agency becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the implementation agency is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the implementation agency takes or suffers any other analogous action in consequence of debt; b. If implementation agency assigns or transfers the contract or any right or interest therein in violation of the provision of contract; or c. If the implementation agency, in the implementation agency, in the	The bidder requests the following modifications: If the bidder fails to perform its obligations (or any part thereof) under this Agreement or if the Agreement is terminated by the Purchaser due to breach of any obligations of the bidder under this Agreement, the Purchaser reserves the right to procure the same or equivalent Goods / Services / Deliverables from alternative sources at the bidder's risk and responsibility. Any such cost borne by the Purchaser in procuring such Goods /Services/ Deliverables shall be borne by the bidder. Any such cost incurred in the procurement of the such Goods /Services/ Deliverables from alternative source will be recovered from the undisputed pending due and payable Payments to the bidder under this Agreement. The cost of procurement from alternate source shall be capped to value of goods/services billed by the implementation agency but not	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
275	14.11.3	121	General terms during termination If the client completes the system, the cost of completing the system by the client shall be determined. If the sum that the implementation agency is entitled to be paid, plus the reasonable costs incurred by the client in completing the system, exceeds the Agreement Price, the implementation agency shall be liable for such excess, limited to the total cost of the project as submitted by the implementation agency. If such excess is greater than the sums due the implementation agency, the implementation agency shall pay the balance to the client, and if such excess is less than the sums due the implementation agency, the client shall pay the balance to the implementation agency. The client and the implementation agency shall agree, in writing, on the computation described above and the manner in which any sums shall be paid	The bidder requests the following modifications: If the bidder fails to perform its obligations (or any part thereof) under this Agreement or if the Agreement is terminated by the Purchaser due to breach of any obligations of the bidder under this Agreement, the Purchaser reserves the right to procure the same or equivalent Goods / Services / Deliverables from alternative sources at the bidder's risk and responsibility. Any such cost borne by the Purchaser in procuring such Goods /Services/ Deliverables shall be borne by the bidder. Any such cost incurred in the procurement of the such Goods /Services/ Deliverables from alternative source will be recovered from the undisputed pending due and payable Payments to the bidder under this Agreement. The cost of procurement from alternate source shall be capped to value of goods/services billed by the implementation agency but not	The criteria is kept as per the criticality of the solution and requirement.
276	14.11	118	Termination	We request OCAC to please add the following termination provision: The bidder may terminate this Agreement, or any particular Services, immediately upon written notice to Client if bidder reasonably determine that bidder can no longer provide the Services in accordance with applicable law or professional obligations.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
277	14.12 Taxes and Duties	121	All payments will be subjected to tax deduction at source as applicable/ required at the prevailing tax rates. Any changes, revision or enactment in duties like GST, taxes or any CESS during the period of validity of the bids and also during the agreement period by Central/State/Other Government bodies will be considered and applied after due consideration. The decision of OCAC in this regard will be final and binding and no dispute will be entertain. Any taxes at the time of supply goods and services shall be applicable as per the Law.	Please confirm :- Any increase in price on account of any statutory increase in or fresh imposition on account of any Tax or Duty leviable in the said Purchase Order, which takes place after the agreed delivery date, shall be borne by Customer. The bidder requests the following modifications: The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately. For purposes of this Agreement, taxes shall include taxes incurred on transactions between Purchaser and the bidder. If, after the last date of submission of this RFP, there is any change of rate of levy under the existing applicable laws of India with respect to taxes and duties or any new introduction of taxes by the Govt, which are directly payable by the Purchaser for providing the services i.e. GST or any such other applicable tax from time to time.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
278	15. Obligations of OCAC	122	Cooling cost, Bandwidth cost, Diesel Cost (if required) and Electricity Cost will be borne by OCAC and this cost is not part of the scope of the bidder. OCAC shall directly engage with these service providers and pay them directly.	We Understand that Electricity Connection charges (One Time Charges) & Recurring charges during Implementation and O&M will be in the scope of OCAC, please confirm. We Understand that Bandwidth, Diesel (if required) charges (One Time Charges) & Recurring charges during O&M will be in the scope of OCAC, please confirm.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
279	15. Obligations of OCAC	122	OCAC would coordinate and assist in acquiring all permissions required for civil construction, earth pit, area for outdoor installations, cooling system, power connectivity from OCAC Tower, back-up power connectivity from OCAC tower	We understand that OCAC shall obtain all requisite statutory clearances prior to commencement of civil and or electrical works, which includes obtaining permissions/consents, Please Confirm. Also we understand that all Right of Way (RoW), Re-Instatement approvals shall be obtained by OCAC by the concerned departments and no extra charges will be paid by the bidder for getting the same in order to complete bidder's obligations, Please confirm.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
280	16.1	123	Exit Management - The exit management period starts, in case of expiry of agreement, on the date when the agreement comes to an end or in case of termination of agreement, on the date when the notice of termination is sent to the successful bidder. - The exit management period ends in three months after the beginning of the exit management period.	The bidder requests the following clarifications: The bidder requests to be compensated for the 3 months of services to be provided during the Exit Management period post expiry of this contract. Please allow the bidder to provide a commercial quote in the financial proposal for the OPEX cost & Manpower costs for 3 months during the Exit Management phase.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
281	Annexure-I : Current asset detail	126	Details of servers installed at the Odisha State Data Centre (OSDC) Details of ESM solution installed at the Odisha State Data Centre (OSDC) , etc Details of devices installed at State IT Centre	Whether the hardware assets listed at SDC, SWAN and State IT Center sites are covered under AMC support (or) not. And please share the validity (EOL/EOS) of all the existing OS & Software licenses. As per pour understanding, the list of all the assests is shared but can you please share th number of devices that would be integrated to the SIEM solution as only the critical infrasturcture will be integrated?	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
282	Annexure – I: Current asset detail	127	Details of ESM solution installed at the Odisha State Data Centre (OSDC)	Do OCAC have a any preference for a SIEM solution from a particular SIEM OEM	All required solution should be as per the minimum technical requirement mentioned in the RFP.

Sl #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
283	Annexure – I: Current asset detail	127	Details of ESM solution installed at the Odisha State Data Centre (OSDC) - Flexconnect -10000 EPS licensed	Bidder understands that existing Arcsight support is valid only till Dec 2021? In case if we are leveraging existing solution, will have to consider additional 10K EPS license for first year and 20k EPS license for rest three years? Is this understanding correct?	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
284	Applications at OSDC	128	List has been provided	Is Application VAPT and Code Review to be conducted for these applications	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
285	List of Devices	126 to 128 and 134 to 137	IT Device List	Is Configuration Review, Rule Review and Compliance Management to be done. We suggest including a solution which will help in the Network Security, Analytics, Rule Management, Configuration Management and Attack Simulation to be included to make the SOC services more complet	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
286	Annexure-I : Current asset detail	136	Assets which are obsolete or approaching obsolescence:	We understand that all obsolete hardware/software located at SDC and SWAN will be replaced by customer after EOS date. Please confirm	The assets in SDC, SWAN and State IT centre are under the authority and discretion of OCAC.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
287	Annexure – I: Current asset detail	137	Events per second generated by the devices at SDC, SWAN and Stata IT Centre Events per second for the existing infrastructure under current scope of work Additional events per second for the proposed additional infrastructure during expansion of CSOC under extended scope of work	We believe that we need to consider estimated events during peak hours for EPS licensing to ensure that the events are not dropped. So, we believe that we need to consider the following EPS volume: 21000 EPS for the existing infrastructure 14000 EPS for the proposed additional infrastructure Events Per Second generated for current infrastructure is given as Avg. 8000 and Peak 21000. Incremental need mentioned is of Avg. 5200 and Peak 14000. Are you expecting this total capacity (Avg - 13200, Peak - 35000) to be available from Day 1 ? What is the volumetric of the Security tickets generated per month by the SOC team	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
288	Proforma 6: Format of Earnest Money Deposit (EMD)	144	In consideration to the advertisement published by OCAC (hereinafter called the "Purchaser") has their offer dated_____ through RFP for Engagement of Agency for Implementation of Odisha Cyber Security Operations Centre at OCAC, Bhubaneswar hereinafter called the "IA") against the purchaser's RFP enquiry No. ____/_____/_____ KNOW ALL MEN by these presents that We _____< Bank Name> of _____ having our registered office at _____ are bound unto _____ (hereinafter called the "Purchaser) in the sum of _____ for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents.	We understand that Referred Offer Dated in EMD Format implies RFP release Date. Please confirm. As per Bank Policies, Bank may add "Notwithstanding anything to the contrary contained herein" clause in the Bank Guarantee. And same shall be acceptable to OCAC .Please confirm. We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both the two conditions, specifying the occurred condition or conditions Notwithstanding anything contained hereinabove: a) Our liability under this Bank Guarantee shall not exceed and is restricted to Rs.	To be modified as per the Letter no. 27928/F FIN-COD-MISC-0008-2017 dated 16-10-2020 from Finance Department.
289	Proforma 10: Authorization letters from all OEMs	150	We abide by the commercials quoted by the Bidder towards AMC charges for four years from the date of supply and successful commissioning of equipment(s) i.e. Go-Live.	We request you to kindly delete this clause from MAF. Since OEM has no control over Bidder's Pricing .It will be challenge for OEM to sign the same. Also for OCAC, Bidder will ensure complete support as per RFP Terms.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
290	Proforma 15	157	1. Price proposal and validity All the prices mentioned in our RFP are in accordance with the terms as specified in the RFP documents. All the prices and other terms and conditions of this RFP are valid for a period of 180 days as desired in the RFP.	The bidder requests the following modifications: All the prices mentioned in our RFP are in accordance with the terms as specified in the RFP documents. All the prices and other terms and conditions of this RFP are valid for a period of 180 days from the last date of submission of the bid as desired in the RFP.	The criteria is kept as per the criticality of the solution and requirement.
291	Proforma 15: Proposal Covering Letter – Financial	157	We hereby confirm that our RFP prices include all taxes. However, all the taxes are quoted separately under relevant sections. We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other corporate Tax in altercated under the law, we shall pay the same. 2. Unit rates We have indicated in the relevant schedules enclosed the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract. 3. Deviations We declare that all the services shall be performed strictly in accordance with the RFP documents except for the variations and deviations , all of which have been detailed out exhaustively in the following statement, irrespective of whatever has been stated to the contrary anywhere else in our proposal.	Kindly amend the clause as: We hereby confirm that our RFP prices include all taxes. However, all the taxes are quoted separately under relevant sections. We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other corporate Tax in altercated under the law, we shall pay the same. 2. Unit rates We have indicated in the relevant schedules enclosed the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract. 3. Deviations We declare that all the services shall be performed strictly in accordance with the RFP documents except for the variations and deviations submitted along with the proposal, all of which have been detailed out	Deviation clause added.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
292	Proforma 16	159	Financial Proposal – IT and Non-IT (CAPEX)	The bidder requests the following modifications: The bidder should be allowed to quote separately for the cost of sale for the IT & Non-IT aseets and also for the Installation & Commissioning costs. The I&C costs should not be bundled along with the supply costs. Under GST regulation, if separate value for hardware, software and services is not defined in the contract, the tax authority may treat entire contract as mixed supply contract. In such cases the highest GST rate applicable for supply is required to be charged to the customer. Thus, it is advisable to define separate value for each deliverable. This will help in reducing compliance issues such as invoicing, e-waybill, time of supply date, etc. further, if any GST rate or new cess levied by Government, the changes can be initiated for separate hardware or asset. Keeping in view of the above, please allow the bidder to quote separately	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
293	Proforma 16	159	Financial Proposal – IT and Non-IT (CAPEX)	The bidder requests the following clarifications: If the bidder plans to use the existing assets (as given in Annexure – I: Current asset detail section of the RFP) and/or upgrade them, is the bidder required to quote for the AMC for 4.5 years of these items also? If yes, please provide an additional proforma to quote for the AMC for the existing assets to be re-used by the bidder. Also provide the payment terms for the upgrade/AMC of these items.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
294	Proforma 16	159	Financial Proposal – IT and Non-IT (CAPEX)	The bidder requests the following clarifications: Is the bidder allowed to bundle the cost of multiple years warranty / AMC along with the supply cost of the IT & Non-IT assets? The vendor/OEMs are also going to do the same and will also be able to provide additional cost benefits which shall be passed on to the purchaser.	The criteria is kept as per the criticality of the solution and requirement.
295	Proforma 16	159	Financial Proposal – IT and Non-IT (CAPEX)	The bidder requests the following clarifications: What is the criteria under which, if needed due to unavoidable circumstances, the bidder change the OEM/Make/Model after the submission of the financial proposal and award of contract?	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
296	Proforma 16 : Non IT Assets (Indicative)	164	42U Rack with 48 port jack pane	1. Is this planned to be put in the HUB Room. Please confirm. 2. In addition if we need additional racks for the IT Hardware where do we plan the same.	Bidder should deploy the Rack in the SOC command centre at the proposed site provided in the RFP.
297	Proforma 17	165	Financial Proposal – Manpower	The bidder requests the following modifications: As the bidder resources will start work from date of award of the contract and will be involved in the various activites of the Implementation phase of the project including Installation & Commissioning of the IT & Non-IT assets, the bidder requests to allow to quote the commercials for the manpower separately for the Implementation phase of the project. If the purchaser so desires, this can be quoted as a fixed price instead of per man month rates for the manpower. Please consider. The bidder requests the following clarifications: Will the manpower resources during O&M phase be considered on a Time & Material basis with monthly attendance to be approved by the Client OR will the manpower costs be considered as a fixed price contract to be billed as Quarterly Guaranteed	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
298	Proforma 18	166	Financial Proposal – Operations and Maintenance (OPEX)	Please allow the bidder to submit the OPEX charges for 1st year also. Else, this severely hampers the cashflow of the deal leading to high finance charges which shall not allow the bidder to propose the best and fair commercial value of the solution.	The criteria is kept as per the criticality of the solution and requirement.
299	Proforma 18	166	Operations and Maintenance Cost estimate for IT asset	Can you please explain how the Operations Maintenance Cost is different than the manpower cost?	The criteria is kept as per the criticality of the solution and requirement.
300	Proforma 20: Financial Proposal – Additional cost	168	User licenses (to be added by bidder) – per device / per user	Please clarify what is User license	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
301	Proforma 21: Letter for self-declaration of clean track record	169	I hereby declare that my company…………………………. has not been debarred / blacklisted by Government of India / Government of Odisha in the last three years for indulging in corrupt or fraudulent practices or for indulging in unfair trade practices and not backed out from executing the work after award of the work as on the RFP submission date. My company…………………………. is also not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this RFP. I further certify that I am competent authority in my company has authorized me to make this declaration.	Kindly amend the below clause as: To the best of our knowledge and as per records available with the Company, I hereby declare that my company…………………………. has not been debarred / blacklisted by Government of India / Government of Odisha in the last three years for indulging in corrupt or fraudulent practices or for indulging in unfair trade practices and not backed out from executing the work after award of the work as on the RFP submission date. As per records available with the Company, my company…………………………. is also not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this RFP. I further certify that I am competent authority in my company has authorized me to make this declaration.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
302	Proforma 22: Format of Bank guarantee	170	Proforma 22: Format of Bank guarantee	The Bank also agrees that this guarantee shall be governed and construed in accordance with Indian Laws and subject to the exclusive jurisdiction of Indian Courts of ~~OCAC~~at _____. This Bank Guarantee issued by _____ Bank, on behalf of the Implementation agency in favor of OCAC is in respect of the Contract/agreement dated_____. As communicated by Implementation agency on the date of execution of this Bank Guarantee an amount of Rupees _____ (Rupees _____ only) is outstanding and payable to Implementation agency by OCAC, in respect of pervious contracts between Implementation agency and OCAC. As communicated by Implementation agency on the date of execution of this Bank Guarantee, there are no outstanding disputes related to any	To be modified as per the Letter no. 27928/F FIN-COD-MISC-0008-2017 dated 16-10-2020 from Finance Department.
303	Proforma 23: Non-Disclosure Agreement	173	Proforma 23: Non-Disclosure Agreement	Kindly remove Proforma 23: Non Disclosure Agreement as all employee have NDA's with the bidder	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
304	General	General	Asset Ownership and transfer of title	The ownership of the assets or goods will be transferred to the Purchaser on the date of delivery of the assets or goods by the bidder to the purchaser's designated carrier for shipment or purchaser's designated location. For each asset, the bidder bears the risk of loss or damage up to the time it is delivered to the Purchaser's designated carrier for shipment or Purchaser's designated location.	The criteria is kept as per the criticality of the solution and requirement.
305	General	General	Contract Extension	The extension and terms of the contract shall be mutually discussed and agreed between the bidder and the purchaser before 3 months of the expiry of the contract. The commercials for extension of the contract beyond the term of the project shall be submitted at the request of the Purchaser.	The criteria is kept as per the criticality of the solution and requirement.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
306	General	General	Acceptance of deliverables	The Purchaser shall provide response or feedback on draft deliverables within 7 working days. Purchaser shall provide signoff within 15 calendar days from the submission of final deliverable in complete form by the bidder. In case, the purchaser fails to provide signoff on the final deliverable within 15 working days, same may be considered as deemed acceptance. However, in case the purchaser confirms to the SI with an alternative date, then that date would stand revised for deemed acceptance. Such revisions will be limited to 1 (one) time for the respective deliverable.	The criteria is kept as per the criticality of the solution and requirement.
307	General	General	General	There are few security solutions for which Gartner/Forrester/IDC/NSS compliance is not mentioned , hence for such cases , Bidder can choose OEM based on Industry standards. Please confirm.	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.
308	General	General	General	Bidder can propose server/compute requirements which may be required for deploying security solutions/Mgmt. consoles as per RFP asks. Please confirm	Bidder to assess the requirement mentioned in the RFP document and propose accordingly.

SI #	RFP Clause No.	RFP Pg #	Existing Clause Details	Query by bidder(s)	OCAC Response / Clarification
309	General	General	General	Please Clarify at which location the security components (Anti APT , SIEM , Log Management Appliance , SOAR , Threat Intelligence feed , Vulnerability Management etc.) needs to be deployed	1. All major SOC solution would be installed at SDC. 2. Limited solutions e.g: UPS, RACK, CCTV, L2 switch, Router, etc. would be installed at SOC command centre. 3. Log management appliance in pairs would be installed at SDC, SWAN and State IT centre. 4. One Anti-APT solution would be installed at State IT centre and One solution at State Data Centre.
310	General	General	General	Kindly Confirm , whether High Availability is to be considered for Security components proposed in RFP.	Redundancy should be planned by the bidder considering the BoM mentioned in the RFP.