ANNEXURE II

RFP Enquiry No.: OCAC-SEGP-INFRA-0009-2019-20016

CORRIGENDUM

RFP NO. RFP ENQ. No.-OCAC-SEGP-INFRA-0009-2019/ENQ-20016 Dated 15.05.2020 Selection of Agency for Supply, Installation & Commissioning of Enterprise Security Solution for Odisha Secretariat LAN.

Important: The corrigendum is to be read, duly signed and submitted along with the original RFP document published on the websites http://www.ocac.in, www.odisha.gov.in and www.tenders.gov.in vide RFP Enquiry No.: - RFP ENQ. No.-OCAC-SEGP-INFRA-0009-2019/ENQ-20016 Dated 15.05.2020

CORRIGENDUM FORMAT

Sl. No.	RFP Clause, Page No, Section	Description of the Clause	Modifications
1	RFP Clause No-6.8, Alternative/ Multiple Bids, Page No-16, Point No-b	The bidder may quote for multiple brands/ make/ model for each item in the technical Bid and should also mention the details of the quoted make/ model of the respective items.	The Clause modified as: - "The bidder must quote single brand / make/ model for each item in the technical bid."
2	Annexure-9, Manufacturer's Authorization Form (MAF) , Page No-49	To be submitted in OEM Letterhead at the time of getting the Purchase Order)	OEM Manufacturer's Authorization Form (MAF) is mandatory and needs to be submitted at the time of bid submission.
3	RFP Clause No-6.21.6, Performance Guarantee, Page No-25	The Performance Guarantee should be valid for a period of 5 years 6 months (66 months). The Performance Guarantee shall be kept valid till completion of the project and Warranty period.	The Clause modified as: - "Performance Bank Guarantee (PBG) should be valid for a period of 3 years & subsequently renewed automatically by Banks for another period of 2 years 6 months (Total 66 months)".

4	RFP Clause No-4.1, Detailed Requirement under this Project, Page No-6, Point No-c	Proposed solution should not be declared with End of Life or End of Support by OEM.	The Clause modified as: - "Along with the OEM MAF the bidder shall submit an undertaking from the OEM, in its official letter confirming that all the spares and software support, including security subscriptions for the quoted products(s) shall be available for purchase (if needed) by OCAC at least for the additional two years calculated from the date of expiry of the contract period as defined in this RFP".
5	RFP Clause No-4.1, Detailed Requirement under this Project, Page No-6, Point No-g	In view of the future integration planned with Odisha SDC, security best practice is to be ensured. Therefore the proposed OEM for the firewall solution at Odisha SEC LAN should not be the same, as of the currently core firewall running in OSDC. This would ensure multi-OEM multi-layered architecture for SEC LAN-SDC communication.	The Clause Deleted.
6	RFP Clause No-4.1, Detailed Requirement under this Project, Page No-8, Point No-m	The Proposed Security Gateway and APT solution must be able to integrate seamlessly and managed from a single dashboard for ease of operation and forensic analysis of security incidents.	The Clause modified as: - "The Proposed Security Gateway and APT solution must be able to integrate seamlessly for ease of operation and forensic analysis of security incidents.
7	RFP Clause No-4.1, Detailed Requirement under this Project, Page No-6, Point No-k	Bidders would be responsible to migrate the existing firewall policies to the new environment.	Existing Firewall Make: Checkpoint, Model: 12200 Next Generation Threat Prevention Appliance (CPAP-SG12200-NGTP).
8	Annexure-3, Minimum Technical Specifications of Enterprise Security Components, Page No-36, Point No-1.05	Solution must support Active-Active redundancy within a single site	The specification modified as: - "Solution must support Active-Active/ Active-Standby redundancy within a single site."
9	Annexure-3, Minimum Technical Specifications of Enterprise Security Components, Page No-36, Point No-1.06	Solution must support adding/removing compute resources without changing security settings and policy. Solution should not be with proprietary ASIC architecture and must be agile, robust and secured in nature	Solution must support adding/removing compute resources without changing Security settings and policy. Solution should not be with proprietary ASIC architecture and should be open architecture based on multi core CPU's to protect & scale against dynamic latest security threats.
10	Annexure-3, Minimum Technical	Solution must provide a linear performance growth and should support at least 25 million concurrent	The specification modified as: - "The Solution should support 15 million concurrent connections

	Specifications of Enterprise Security Components, Page No-36, Point No-2.01	connections from day 1 and scalable to support 40 million without any additional cost.	from the day 1 and scalable to 30 million".
11	Annexure-3, Minimum Technical Specifications of Enterprise Security Components, Page No-36, Point No-2.03	Solution must be able to provide an overall throughput of at least 20 Gbps scalable to 4 times in future in case the asked minimum throughput is not sufficient to cater to the user traffic. Solution should be modular and must have provision to add similar gateway modules to have linear growth of performance without replacing the existing ones. Additional modules would be purchased by Orissa Secretariat LAN separately based on authentic data point provided by the SI. The throughput should be measured under typical enterprise traffic condition combining traffic patterns, like HTTP, HTTPS, SMTP, Telnet, DNS, SQL etc. with multiple packet sizes ranging from 10K up to 500K.	The specification modified as: -"Solution must be able to provide an overall throughput of 20 Gbps or higher, from the day 1 after enabling all modules under typical enterprise traffic condition combining traffic multi-protocol traffic mix with multiple packet sizes".
12	Annexure-3, Minimum Technical Specifications of Enterprise Security Components, Page No-39, Point No-4.03	The detailed report must include: a) screenshots, b) timelines, c) registry key creation/modifications, d) file and processes creation, e) Network activity detected.	The specification modified as: - "The system should be capable of generating reports relating to URL filtering, Content filtering, Threats, Data filtering, unknown malware analysis, Authentication, Tunneled Traffic etc. "
13	Annexure-3, Minimum Technical Specifications of Enterprise Security Components, Page No-37, Point No-6.05	The solution should support deployment in both inline and TAP mode. Minimum interfaces to be proposed – 4 x 1G, RJ45 and 2 x 10G, SFP+ interfaces. Should be supplied with redundant power supply.	The specification modified as:-"The solution should support deployment in both inline and TAP mode. Minimum interfaces to be proposed – 2 x 1G, RJ45 and 2 x 10G, SFP+ interfaces. Should be supplied with redundant power supply".
14	Annexure-3, Minimum Technical Specifications of Enterprise Security Components, Page No-38, Point No-3.15	50 SSL Client Licenses are available from day one. However the solution supports unlimited SSL client licenses.	The specification modified as:-"Zero Trust Network Access (ZTNA) or Software Defined Perimeter (SDP) integrated with Multifactor Authentication Solution should be proposed for private apps with minimum of 50 zero trust client licenses from day-1 and scalable to support 10k zero trust client licenses. Proposed OEM must listed in Gartner's Market Guide for Zero Trust Network Access

			Representative Vendor Category, any hardware required to meet the solution to be provided from day-1 with each level of redundancy, Proposed Architecture should be such that, the zero trust clients should connect to the Gateway using Single Packet Authorization (SPA) protocol followed by mutual TLS protocol and if both Single Packet Authorization and mutual TLS are successful, the ZT Gateway accepts the connection and provides access to the application / service for identifying the actual user without additional authentication".
15	Annexure-3, Minimum Technical Specifications of Enterprise Security Components, Page No-41, Point No-6.06	The emulation engine should be able to inspect, emulate, prevent and share the results of the sandboxing event into the anti-malware infrastructure. The Sandboxing solution should have cloud redundancy with equivalent Sandboxing throughput of 4000 files per hour. The solution should support addition of sandbox appliance in case the current appliance is not sufficient to emulate the amount of unique files generated in Orissa Secretariat LAN network. Additional appliance would be procured separately.	The specification modified as:-"The engine should be able to inspect, emulate, prevent and share the results of the sandboxing event into the anti-malware infrastructure. The Sandboxing solution should have cloud redundancy with equivalent Sandboxing throughput of 1000 files or more per hour. The solution should support addition of sandbox appliance in case the current appliance is not sufficient to emulate the amount of unique files generated in Odisha Secretariat LAN Network, with additional appliances (if, any) to be included".
16	Annexure-3, Minimum Technical Specifications of Enterprise Security Components, Page No-41, Point No-6.11	The solution should have anti-evasion capabilities detecting sandbox execution. The solution must be able to detect ROP and other exploitation techniques (e.g. privilege escalation) by monitoring the CPU flow at the network.	The Clause modified as: - "The solution should have anti-evasion capabilities detecting sandbox execution. The solution must be able to detect exploitation and zero day threats".
17	Annexure-3, Minimum Technical Specifications of Enterprise Security Components, Page No-37, Point No-3.01	The OEM must have security effectiveness proven over the years and must be rated as leaders in the Gartner MQ for enterprise firewall in the last three years and must have received a recommendation equal to or greater than 95% in the Security Value Map for Next Generation Firewall from NSS Labs in 2019.	The specification modified as: - "The OEM must have security effectiveness proven over the years and must be rated as leaders in the Gartner MQ for enterprise firewall in last three years".

Annexure-2: Indicative Bill of Quantity (BOQ)

Sl. No.	Item Details	Offered Make & Model (to be filled in by the bidder)	UoM	Qty
1	Next Generation Firewall (NGFW) in High Availability (HA)		Set	01
2	10G Base SR SFP+ Transceivers		Nos	12
3	Management & Reporting hardware appliance and software/license for NGFW		No.	01
4	Anti-APT Sandboxing solution (On Premise with Hardware + Software and licenses)		Set	01
5	Zero Trust Network Access (ZTNA) solution (on premise with Hardware / Software)		Set	01
6	Zero trust client Licenses		Nos	50
7	Optical Patch Cable, OM4 Multi-mode mode, Duplex LC-LC, 10 meters (Commscope/Panduit/Belden)		Nos	20
8	CAT6 UTP Patch Cord – Factory Crimped, 3 meters (Commscope/Panduit/Belden)		Nos	10
9	CAT6 UTP Patch Cord – Factory Crimped, 10 meters (Commscope/Panduit/Belden)		Nos	10
10	Cisco SFP-10G-SR module (Part Number : SFP-10G-SR)		Nos	04
11	Radware (Alteon D-6024) SFP-10G-SR module		Nos	04

Annexure-11: Commercial Bid - Item Wise Price Schedule

Sl. No.	Item Description	Qty	Unit	Base Product Cost Including 5 Years OEM Support	Base Installation cost	Unit Price	GST Charges as applicable	Total Product Cost (Including GS
1	**2**	**3**	**4**	**5**	**6**	**7=5+6**	**8**	**9=7+8**
1	Next Generation Firewall (NGFW) in High Availability (HA)	01	Set					
2	10G Base SR SFP+ Transceivers	12	Nos					
3	Management & Reporting hardware appliance and software/license for NGFW	01	No.					
4	Anti-APT Sandboxing solution (on premise with Hardware + Software and licenses)	01	Set					
5	Zero Trust Network Access (ZTNA) solution (on premise with Hardware / Software)	01	Set					
6	Zero trust client Licenses	50	Nos					
7	Optical Patch Cable, OM4 Multi-mode mode, Duplex LC-LC, 10 meters (Commscope/Panduit/Belden)	20	Nos					
8	CAT6 UTP Patch Cord – Factory Crimped, 3 meters (Commscope/Panduit/Belden)	10	Nos					
9	CAT6 UTP Patch Cord – Factory Crimped, 10 meters (Commscope/Panduit/Belden)	10	Nos					
10	Cisco SFP-10G-SR module (part number : SFP-10G-SR)	04	Nos					
11	Radware (Alteon D-6024) SFP-10G-SR module	04	Nos					
							GRAND TOTAL	
Grand Total In Word:								

Note:

- **All the above price would be in INR only.**
- **The above price would include Compressive OEM Warranty Support for a period of 5 years from the date of UAT.**
- **The bidder has to compulsorily quote for all items mentioned in the Commercial-bid Tables. In case bidder fails to quote for any of this stage, the bid would be summarily rejected.**
- **Above is indicative, however the quantity may increase or decrease at the time of placing the purchase order as per actual.**
- **The Tax rates will be mentioned as per standards.**