# WEBEL TECHNOLOGY LIMITED

## Corrigendum -I

## WTL/NKGS/ICCC/20-21/024 dated 26.02.2021

| Sl No. | Section No. | Clause No. | Page No. | clarification sought | WTL Remarks |
|---|---|---|---|---|---|
| 1 | 1.1.3.1 Functional Specifications of the Application Software | | 143 | The System shall support on-demand or automatic outgoing call initiation.<br>a) The SMS shall maintain an electronic telephone book that may be searched or used for on-demand calling.<br>b) Calling capability shall be available via GIS map icons.<br>c) SIP protocol shall be supported.<br><br>We are assuming that there is an existing database for electronic telephone book which will be intergrated to the ICCC and the client will provide the SIP server / telephony API for integration. Is our assumption correct ? If yes, please provide the details. | The existing address book maybe available in a structured or non-structured format. |
| 2 | Section A: | 1.2 SCOPE OF WORK | 23 | **Content in the RFP:**<br>The Data Centre will be housed by using the existing State Data Centre at Monibhandar<br><br>**Clarification Required:**<br>Please brief the MSI scope of work at State data center at Monibhandar. | MSI shall need to submit the requisite details Connectivity, configuration and connection to ICCC is in scope of bidder. |

| | | | | | |
|---|---|---|---|---|---|
| 3 | Section A: | 1.2 SCOPE OF WORK | 23 | **Content in the RFP:**<br>The Data Centre will be housed by using the existing State Data Centre at Monibhandar<br><br>**Clarification Required:**<br>As per our understanding, WBSDC authorities will provide enough rackspace as per bidder's requirement & other basic amenities like physical/logical security, fire proof system, cooling, power, bandwidth, internet etc.. to host required IT hardware at SDC as per RFP solution. Please confirm. | MSI shall need to submit the requisite details Connectivity, configuration and connection to ICCC is in scope of bidder. |
| 4 | Annexure 1 | 5.1.3.2.1 Security Services for CCC solution | 158 | **Content in the RFP:**<br>The proposed solution should have a Business Continuity Plan and a Disaster Recovery Plan prepared and implemented by the SI before commencement of the operations. Robust backup procedures to be established for the same.<br><br>**Clarification Required:**<br>What is the DR compute & storage capacity to be considered. | As per tender |
| 5 | Annexure 1 | 5.1.3.2.1 Security Services for CCC solution | 158 | **Content in the RFP:**<br>The proposed solution should have a Business Continuity Plan and a Disaster Recovery Plan prepared and implemented by the SI before commencement of the operations. Robust backup procedures to be established for the same.<br><br>**Clarification Required:**<br>Please confirm who will provision the network connectivity between DR to SDC & DR to ICCC locations so that DR will take over in failover conditions. | Scope of bidder |

| | | | | | |
|---|---|---|---|---|---|
| 6 | Annexure 1 | 37 Switch & router networking | 121 | **Clarification Required:**<br>Please provide router specs. Which are missing from the section. | Description Minimum Specifications Change Requested<br>Wireless Interface IEEE 802.11b/g/n 2.4GHz wireless IEEE 802.11b/g/n/ac Wave 2 5GHz wireless IEEE 802.11b/g/n 2.4GHz wireless IEEE 802.11b/g/n/ac Wave 2 5GHz wireless MIMO 2 x 2 2 x 2 Data Rate 2.4 GHz - Up to 400 Mbps 5 GHz (1) - Up to 867 Mbps 5 GHz (2) - Up to 867 Mbps 2.4 GHz - Up to 400 Mbps 5 GHz (1) - Up to 867 Mbps 5 GHz (2) - Up to 867 Mbps<br>Antenna Internal omnidirectional antennas 2.4 GHz: 3 dBi 5 GHz: 4 dBi Internal omnidirectional antennas 2.4 GHz: 3 dBi 5 GHz: 4 dBi<br>Operating Frequency 2400 to 2483.5 MHz 5150 to 5850 MHz 2400 to 2483.5 MHz 5150 to 5850 MHz<br>Operating Channels 1 to 13 channels for 2.4 GHz band (per country code) 36 to 165 channels for 5 GHz band |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | (per country code) 1 to 13 channels for 2.4 GHz band (per country code)<br>36 to 165 channels for 5 GHz band (per country code)<br>Ethernet Interface 2 x 10/100/1000BASE-T LAN port 2 x 10/100/1000BASE-T LAN port |
| 7 | Annexure 1 | 5.1.3.2.1.1 Intrusion Prevention System (IPS) | 158 | **Clarification Required:**<br>Minimum specifications provided in RFP for IPS are very open ended and basic. Please provide detail specs. And also this line item is not mentioned in the BOM, please add. | As per tender |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Annexure 1 | 39. ICCC/TR/3 9.0 1 - 960GB SSD SATA & Redhat OS | 122 | **Clarification Required:**<br>Please make changes as "960GB SSD SATA or SSD" as SSD drives can be used for faster performance and "Redhat or any other OS" as OS is limited to particular OEM. Every application runs in different OS. | Redhat is the only available OS at the SDC |
| 9 | Annexure 1 | 35. Smart rack - U space available for IT Load 22 U | 119 | **Clarification Required:**<br>Please make changes as "22 U or 42 U" as 22 is not available in market and 42 U is appropriate for the requirement | it is mentioned minimum space requiered for IT load. |
| 10 | Annexure 1 | ICCC/TR/1 4.3 Voice Recordings | 91 | **Clarification Required:**<br>Please confirm us the retention period for voice recordings to arrive the storage sizing. | For the period till the end of maintenance |

| | | | | | |
|---|---|---|---|---|---|
| 11 | Annexure 1 | 3a, Solution & Platform: | 139 | **Content in the RFP:**<br>Integration of up to 2500 CCTV Camera Live Feed at the ICCC from Network connected CCTV Camera. The same should be viewed on real-time with at least 250 camera feed to be projected onto the Video-wall at any given time.<br>Note : The bidder shall not get any form of direct access to the existing VMS. They shall be provided with only a feed via a network. The interpretation of that feed and needful display of the same shall require appropriate equipment (VMS or others) to display.<br>Such solution and infrastructure should be a designed to support up to 2500 CCTV feeds<br><br>**Clarification Required:**<br>ICCC is a thin client model cannot handle 250 cameras live feed on web based application. Hence, request to amend the clause as follows.<br><br>Integration of up to 2500 CCTV Camera Live Feed at the ICCC from Network connected CCTV Camera.<br>Thin client of command center should be able to handle upto 100 cameras live feed and thick client should be able to handle upto 250 cameras live feed to be projected onto the Video Wall at any given time. | As per tender |

| | | | | | |
|---|---|---|---|---|---|
| 12 | F | 2.4 Design, Build and Maintenance of Integrated Command and Control Centre Or Data Centre Or any Project on IOT | 53 | Ongoing Project credentials have been considered in pre qualification(PQ), we understand that on-going project credentails shall also be applicable for technical qualification (TQ) of bidder.<br>; Documentary evidence (Copy of completion/ Ongoing client certificate and Work Order/ Contract) shall be presented. | will be considered |
| 13 | F | 2.5 Data Centre & WAN experience Or IOT | 54 | Request for clarification whether any single project of 100 Cr is required or cumulative projects shall be considered equating to 100 Cr in the last 5 years amongst the options presented. Also if we submit a combination of projects amongst the option presented, will that be considered for a technical score. | cumulative figure can be considered |
| 14 | ICCC/TR/36.01 - Technical Requirements - OFC cabling & Laying from SDC to ICCC | | 119 | As pe the norms of the respective authorities, there is a separate charge as lease rental for a period of 5 years ( ), since our project duration if for 3 years, it is requested to bear the lease rental charges and exclude from bidder scope. | To be considered |
| 15 | Section Q - Manufacturer Authorization Form | | 71 | Request to consider MAF issued during 1st Call | MAF transferable from 1st call but OEM should atleast give a declaration with the mention of the new tender number with adhereance to the earlier MAF |
| 16 | ICCC/TR/4.12 to ICCC/TR/4.16 | | 77 | The "Cube Management" is specific OEM capability. Request the same to be made optional for allowing other OEMs to participate | To be considered as optional |

| | | | | | |
|---|---|---|---|---|---|
| 17 | ICCC/TR/14.<br>21 - EPABX<br>SYSTEM | | 97 | **Mentioned in Tender:** Alternatively may support Cloud TelephonyMentioned in Tender: Alternatively may support Cloud Telephony<br>based IVR, Call Recording, Integration<br><br>**Query:** Would like to clarify if the this means that the EPABX system feature can alternatively be supported through cloud based solutions as well | Cloud telephony based equivalent solution is accepted |

| | | | | | |
|---|---|---|---|---|---|
| 18 | ICCC/TR/25.01 | | 109 | General<br>• Should be a purpose built appliance based solution with integrated functions like Firewall, VPN and User awareness. The product licensing should be device based and not user/IP based (should support unlimited users except for VPN). The hardware platform & Firewall with integrated SSL/IPSec.<br>• Should have minimum 40 Gbps throughput, and should be able to handle all peakloads. Throughput capacity of VPN should not be less than 15 Gbps<br>• Should support Max 2,50,00,000 concurrent sessions for data.<br>• Should support atleast 1,00,000 connections per second.<br>• Should be based on multi core processors and not on proprietary hardware platforms like ASICs, Should have minimum 16 GB memory with option of upgradable to 64 GB or more. Hardware should have field upgradable capabilities for upgrading components like network cards, RAM, power supplies, fan etc.<br>• Solution should have following deployment modes mandatory: a) L3 Mode, b) L2/Transparent Mode.<br>• Should be deployed in High Availability.<br>• Should support hardware fail open cards for critical interfaces and appliances level.<br>• NGFW appliance should have inbuilt storage of 250 GB or more SSD / HDD. 8 x 10/100/1000 Base-T Copper Ports, 4 x 10G SFP ports from day 1 and support<br>For | Minimum Requirement<br>• Should have minimum 40 Gbps throughput, and should be able to handle all peakloads. Throughput capacity of VPN should not be less than 3 Gbps<br>• Should support Max 1,00,00,000 concurrent sessions for data.<br>• Should support atleast 1,30,000 connections per second.<br>• Should be based on multi core processors and not on proprietary hardware platforms like ASICs, Should have minimum 12 GB memory.<br>•NGFW appliance should have inbuilt storage of 240 GB or more SSD / HDD. 8 x 10/100/1000 Base-T Copper Ports ,2 x 1G SFP & 2 x 10G SFP+ ports from day 1 and support for addition of 2 x 40G SFP/ 4 X 10 G SFP+ ports. |

| | | | | | |
|---|---|---|---|---|---|
| 19 | ICCC/TR/25.02 | | 110 | Firewall Feature:<br>• Should be based on "stateful inspection" technology and should support access control for at least 500 predefined/services/protocols with capability to define custom services.<br>• The communication between the management servers and the security gateways should be encrypted and authenticated with PKI Certificates | Minimum Requirement<br>Firewall Feature:<br>• Should be based on "stateful inspection" technology and should support access control for at least 500 predefined/services/protocols with capability to define custom services.<br>• The communication between the management servers and the security<br>gateways should be encrypted and authenticated with PKI Certificates |

| | | | | | |
|---|---|---|---|---|---|
| 20 | ICCC/TR/25.03 | | 110 | Authentication<br>• Support by the security gateway and VPN module: tokens (i.e. Secure ID), TACACS, RADIUS and digital certificates. Should support Ethernet Bonding functionality for Full Mesh deployment architecture.<br>• Should support user, client and session authentication methods. User authentication schemes should be supported by the security gateway and VPN module: tokens (i.e. -Secure ID), TACACS, RADIUS and digital certificates.<br>• Firewall should support the system authentication with RADIUS and local authentication. Both should work simultaneously.<br>Solution should support DCHP, server and relay.<br>• Solution shall include the ability to work in Transparent/Bridge mode. | Minimum Requirement:<br>Authentication<br>• Support by the security gateway and VPN module: tokens (i.e. Secure ID), TACACS, RADIUS and digital certificates. Should support Ethernet Bonding functionality for Full Mesh deployment architecture.<br>• Should support user, client and session authentication methods. User authentication schemes should be supported by the security gateway and VPN module: tokens (i.e. -Secure ID), TACACS, RADIUS and digital certificates.<br>• Firewall should support the system<br>authentication with RADIUS and local |
| 21 | ICCC/TR/25.04 | | 110 | High Availability<br>• Solution shall support gateway high availability and load sharing with state synchronization.<br>• Solution shall support configuration of dual stack gateway on a bond interface or on a sub-interface of a bond interface. Solution should Support 6 to 4 NAT, or 6 to 4 tunnel. | Solution shall support configuration of dual stack gateway on a bond interface or on a sub- interface of a bond interface. Solution should Support 6 to 4 NAT, or 6 to 4/6 in 4 tunnel |

| | | | | | |
|---|---|---|---|---|---|
| 22 | ICCC/TR/25.05 | | 110 | User Identity / Awareness<br>• Should be able to acquire user identity from Microsoft/Linux Active Directory without any type of agent installed on the domain controllers.<br>• Should support Kerberos transparent authentication for single sign on.<br>• Should support the use of LDAP nested groups.<br>• Should be able to create rules and policies based on identity roles to be used across all security applications.<br>• Should have the inherent ability to detect multi-stage attacks.<br>• Should include static analysis technologies like antivirus, antimalware/anti bot however in an integrate mode with the solution.<br>Security<br>• Should inspect the web sessions (HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the internet. Third Party/Separate appliance for SSL offloading will not be accepted.<br>• The proposed solution should dynamically generate real-time malware intelligence for immediate local protection via integration with the separate Automated Management and Event Correlation System.<br>• Solution should have an ability to remove all the active content, macros, block the malicious contents while sending document to the end user as clean document.<br>• Solution should have n Multi-tier engine to detect & prevent Command and Control IP/URL and DNS.<br>• Solution should be able to detect & prevent unique communication patterns used by BOTs i.e. Information about Botnet family.<br>• Solution should be able to detect & prevent attack types i.e., such as spam sending click fraud or self-distribution, that are associated with Bots. | Bidders must supply an Anti-APT platform covering Web & Network infection vectors, as a dedicated purpose-built solution to be deployed independently without any functional reliance on existing or 3rd party security solutions.<br>Proposed APT solution should be designed as independent of other layers of security such as firewall , IPS, WebProxy, Anti-Spam or Anti Virus solutions, in a scenario, if any of these layers are replaced or non-functional at certain point of time, the proposed APT solution should be capable of working independently without any dependencies.<br>The proposed APT solution must detect zero- day, multi-stage, file-less, multi-flow and other evasive advanced attacks using dynamic, signature-less analysis in a safe, anti-evasive execution environment. The solution must be sized appropriately by the bidder with no additional costs to achieve performance, scalability, and sizing required to run the proposed solution during entire project project period.<br>Proposed Web APT solution should also have SSL Intercept capability to examine encrypted user bound traffic to detect threats (such as |

| | | | | | |
|---|---|---|---|---|---|
| | | | | • Solution should be able to block traffic between infected Host and Remote Operator and not to legitimate destination.<br>• Solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc. | CnC traffic and data exfiltration) that attackers may hide in encrypted streams. If solution does not have native SSL capability, 3rd party SSL solution must be factored.<br>The proposed solution must stop the infection, |