RailTel Corporation of India Ltd

(A Government of India Enterprise)

Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar,
New Delhi-110023

Website: **www.railtelindia.com**

No. RailTel/Tender/OT/CO/DNM/BW Hiring/2021-22/01 dated 30.07.2021

Corrigendum-1

Subject: Hiring of Bandwidth

Ref : This Office Tender No. RailTel/Tender/OT/CO/DNM/BW Hiring/2021-22/01 dated 15.07.2021

1. **Bidder may submit "Bid Security Declaration" in lieu of EMD. Following clause is added:**

   In lieu of Bid Security/Earnest Money Deposit (EMD) bidder may submit "Bid Security Declaration" in the format given as Annexure-1 ,accepting that if they withdraw or modify their bids during period of validity etc., they will be banned for the period of Three years.

2. **Clause Number 3.4.1 is added Scope of Work (SOR B)as under:**

   3.4.1 : The Bidder shall provide /28 Public IP Pool along with 80 Mbps Intern Leased Line link.

3. **Clause number 3.3.3 - " DDoS Technical Requirements" under Clause 3.1 "Scope of work (SOR A)" is added as under:**

   a) DDoS attacks of capacity up to 20 Gbps, however the capacity shall be increased in case of requirement.
   b) Protection from DDoS attack shall be done using any of the following methods:

      i) TCP/UDP based policy
      ii) BGP blackholing
      iii) Block IP addresses/Geolocations
      iv) Rate limiting of specific/range of IP Address

   c) DDoS Mitigation platform shall support BGP flow spec to mitigate the DDoS attacks.

   d) The solution shall be able to detect and mitigate volumetric DDoS attacks against applications, websites, web forms, email, file transfer or DNS services and other emerging attacks.

   e) The DDoS mitigation service shall be capable of mitigating volumetric, state exhaustion, L-3 & L-4 attacks like:
      a. UDP/ICMP Floods

b. SYN Floods
c. TCP Flag Abuses
d. GET/POST Floods
e. DNS Reflection
f. DNS Flood Attack
g. HTTP Flood
h. Zero Day Attacks
i. ICMP flood
j. Ping of death
k. IP fragmented attack

f) The DDoS mitigation service shall use past traffic pattern to differentiate between legitimate and malicious traffic (Statistical anomaly based attack detection) and legitimate users shall not get affected during attack mitigation. The solution shall automatically learn and adapt to changes in customer's traffic profile and identify/mitigate attacks accordingly.

g) The DDoS service shall support automatic mitigation i.e. Mitigation process shall automatically start once DDoS attack is detected by Service provider and duly inform to customer

h) RailTel will mitigate attacks using their mitigation/scrubbing centres in India.

i) The DDoS mitigation service shall support BGP diversion to redirect traffic during a DDoS attack to scrubbing centre's to filter out malicious traffic and allow only clean traffic towards customer.

j) DDoS mitigation solution shall have ability to block traffic based on specific botnet signatures and Global threat intelligence feed derived from the OEM.

k) The solution shall support detection and mitigation of IPv4 attacks.

l) Detailed reports indicating attack & mitigation details shall be shared by service provider. Reports shall be provided after every mitigation event including specific details about the event, date, time, traffic passed and dropped. The service provider shall provide details like techniques used to block the attack traffic, their configuration settings etc. how much traffic was passed and dropped by each technique etc.

m) In-depth reporting and online user portal shall be provided for:
   (a) Real-time monitoring and statistics of malicious activity, threats and attacks.
   (b) Ability to view attack activities based on continent and countries.
   (c) Ability to monitor and highlight recent new and growing threats.

n) Solution manage portal is accessible only RailTel network or through VPN only.

o) No additional hardware will be installed at customer site for DDoS service

4. All other terms and conditions remain same as per LT Document.

Naresh Kumar
DGM/IT
For & on behalf of
RailTel Corporation of India Ltd.

Annexure-1

Format for Bid Security Declaration
(On Non-judicial stamp paper of Rs. 100/-)

Whereas, I/We _____(Name of Agency) has submitted bid for _____ (Name of Work and Tender No.) and whereas Earnest Money Deposit is being exempted in the aforesaid tender to give relief to the bidders as per Govt. of India guidelines due to severe financial crunch on account of slowdown in the economy due to the pandemic,

I/We hereby submit the following "Bid Security Declaration" in lieu of exemption from submitting Earnest Money Deposit :-

1) If I/We withdraw or modify my/our bid during the bid validity period (including extended validity of tender) specified in the tender documents;

Or

2) If, after the award of work, I/We fail to accept LOA/LOI, or to sign the contract agreement or fail to submit performance guarantee or fail to commence the work within stipulated time period prescribed in tender documents;

Or

3) If I/We furnish any incorrect or false statement / information/ document;

Or

4) If I/We hide any relevant information or do not disclose any material fact in the tender;

Or

5) If I/We commit any breach of integrity Pact;

I/We may be disqualified and banned for a period of three years and shall not be eligible to bid for future tenders in RailTel Corporation of India Ltd. for the period of three years from date of issue of such orders.

(Signed by the Authorized Representative of Firm).

Name of Authorized Representative

Name of Firm

Date