CORRIGENDUM No.2

Corrigendum no. 2 dated 31.12.2021

Tender no. GEM/2021/B/1739100 Dated: 07-12-2021

Name of the Work: Supply Installation and Integration of DDoS appliance.

Item Description	**To be Read as**
Bid opening date/Time 28.12.2021 15:30:00	**07.01.2022 15:30:00**

DDoS POC TESTING AT SECUNDERABAD Data center

Bidder for Anti DDoS solution has to perform a POC setup at Secunderabad Data Centre which includes OEM Hardware with all necessary software's/Licenses and tools(Hardware/Software) required for testing and successful POC along with OEM technical engineer available at POC site.

The RailTel will provide the following infra and support.

1. Rack space in data center
2. Power output -C13-14 connector
3. Cooling
4. Internet Bandwidth
5. If any VM required

The bidder has to arrange tools for generating traffic and hardware to perform and demonstrate the following test at RailTel Secunderabad data centre during POC period for compliance audit.

Failure to conduct POC or failure to demonstrate any item of POC may lead to bid getting technically disqualified.

Sl no	**Test Cases**	**Test Description**	**Compliance /Non-Compliance**
1	DDOS Appliance	1)OEM should Showcase by deploying appliance in production/ test environment in transparent mode, it should not hold any ip address on its interface.	

2	Zero Day Attack Protection with Automatic Signature Generation in less than 30 Seconds.	ZERO DAY ATTACK PROTECTION should be provided by behaviour-based protection with automatic signature creation within 90 seconds of unknown, zero-day DDoS attacks. Bidder and OEM should Showcase by Blocking Attacks based on the Footprint of the attack.	
	Showcase Security Policies:	Device should have Various Security Filters to Protect Against any known and Unknown DDoS Attack. Bidder and OEM should Showcase Options to Configure Security Policies. 1. TCP SYN FLOOD / Anti-Scanning Protection 2. Behavioural DoS Protection 3. DNS Flood Protection 4. Signature Protection, 5. SYN Flood Protection 6. Traffic Rate protection	
	Showcase ACL based Policy Creation.	Device should have functionality to create Blacklist and White List. Bidder and OEM should Showcase Options to Configure Black List and White List.	
	Showcase Network-flood protection should include:	Device should Provide Protection Against all Network Floods. Bidder and OEM should Showcase protection against Network Flood Protection. 1. TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood 2. UDP flood 3. ICMP flood	
	Showcase Advance DNS Based DDoS Protection for All Query type.	Device should Provide Protection Against DNS Based DDoS Attacks. Bidder and OEM should Showcase Options to Configure DNS Based DDoS Attack Protection. 1. A Query. 2. MX Query 3. PTR Query 4. AAAA Query	

		5. Text Query 6. SOA Query 7. NAPTR Query 8. SRV Query 9. Other Queries	
	Reporting and Centralized Monitoring.	The proposed solution should have Centralized Management, Monitoring, and Reporting Module for Single pane of Glass Operations. Bidder and OEM should Showcase reporting and Monitoring Module capabilities.	
All other terms and conditions of tender remain the same.			