GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1225
TO BE ANSWERED ON: 16.12.2022

CYBER SECURITY CHALLENGES ON ROLL OUT OF 5G SERVICES

1225. DR. K. KESHAVA RAO:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether Government has identified possible cyber security challenges on the rollout of 5G network services in the country, if so, the details thereof.
(b) whether the current cyber security infrastructure in the country is enough to tackle future security threats, if so, the details thereof; and
(c) the steps Government is planning to increase the cyber security infrastructure in the country in order to tackle possible future threats?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): Yes sir. The Government is fully aware of both opportunities and cyber security challenges on the rollout of 5G network services in the country. The following measure shave been taken to deal with such challenges:

(i) Telecom services in India are provided by Telecom Service Providers (TSPs) after obtaining license from the Department of Telecommunications (DoT). For ensuring security of telecom networks, the TSP has to abide by the security conditions specified in the license agreement, which are technology-agnostic. As per these terms and condition, licensees are required to annually get their networks audited for security from a network audit and certification agency. The licensees are solely responsible for security of their networks.
(ii) DoT has notified the Indian Telegraph (Amendment) Rules, 2017, enabling mandatory testing and certification of telecommunication equipment. These prescribe that any telegraph which is used or capable of being used with any telegraph established, maintained or worked under a licence granted by the Central Government under the Indian Telegraph Act, 1885 has to undergo, prior to sale, mandatory testing and certification in respect of parameters determined by the telegraph authority.
(iii) The National Security Directive on the Telecommunications Sector mandates TSPs to procure and deploy trusted product only from trusted sources.
(iv) The Telecom Security Operation Centre has been developed for monitoring the security of the telecommunication network in the country. It monitors metadata, with a view to detect any anomaly in the traffic leading to a telecom security incident proactively and take appropriate action.
(v) The Government has established a National Centre for Communication Security at Bengaluru, which has been entrusted with the responsibility of drafting the Indian Telecom Security Assurance Requirement. 11 Security Assurance Requirements have been issued by the Centre for different core elements of 5G.

(b) and (c): Yes sir. Cyber security capabilities and infrastructure are continuously expanding. The Government has taken following steps to increase the cyber security infrastructure in the country in order to tackle possible future threats:

(i) The Indian Computer Emergency Response Team (CERT-In) has set up the National Cyber Coordination Centre to generate situational awareness regarding existing and potential cyber security threats.

(ii) To protect sensitive information, the National Informatics Centre (NIC) adopts a layered security approach, in the form of practices, procedures and technologies put in place on both the network and application levels. This is strengthened through periodic compliance, audit and vulnerability assessment.

(iii) The analytics centre at National Critical Information Infrastructure Protection Centre provides near-real-time threat intelligence and situation awareness, based on which regular alerts and advisories are sent to critical information infrastructure / protected system entities to mitigate cyber security threats.

(iv) The Department of Science and Technology has established a national mission on interdisciplinary cyber physical systems, under which 25Technology Innovation Hubs have been set up in advanced technologies in premier institutes of national importance. One of these hubs, in the technology vertical of cyber security and cyber security for physical infrastructure, is set up at Indian Institute of Technology Kanpur.

****