GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

RAJYA SABHA
STARRED QUESTION NO. 203
ANSWERED ON 06TH AUGUST, 2026

SECURITY AND RESILIENCE OF TELECOM NETWORK INFRASTRUCTURE

203 SHRI AKHILESH PRASAD SINGH:

Will the Minister of Communications be pleased to state:

(a) whether Government has undertaken a comprehensive review of resilience of India's telecom infrastructure against cyber-attacks, network failures and natural disasters;

(b) whether existing telecom security standards are adequate to address emerging technological threats;

(c) the measures taken to improve network redundancy, emergency communication systems and infrastructure resilience; and

(d) whether a national telecom resilience policy is under consideration?

ANSWER

MINISTER OF COMMUNICATIONS AND DEVELOPMENT OF NORTH EASTERN REGION
(SHRI JYOTIRADITYA M. SCINDIA)

(a) to (d) A statement is laid on the Table of the House.

STATEMENT TO BE LAID ON THE TABLE OF RAJYA SABHA IN RESPECT OF PARTS (a) TO (d) OF THE RAJYA SABHA STARRED QUESTION NO. 203 FOR 06th AUGUST, 2026 REGARDING "SECURITY AND RESILIENCE OF TELECOM NETWORK INFRASTRUCTURE"ASKED BY SHRI AKHILESH PRASAD SINGH.

(a): The telecommunication infrastructure, through a comprehensive framework, has been reviewed in consultation with various stakeholders, assessing network resilience against cyber-attacks, network failure and natural disasters. Based on the same, necessary provisions have been made in the law. The Telecommunications Act, 2023 provides for measures towards telecommunication infrastructure resilience. Pursuant to the said provisions, the Telecommunications (Telecom Cyber Security) Rules, 2024, the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024 and the Telecommunications (Standards, Conformity Assessment and Certification) Rules, 2025 have been made. Under provisions of these rules, telecommunication entity maintains a telecom cybersecurity policy and undergo audits to evaluate network resilience and implement necessary safeguards, while verifying that telecom equipment complies with essential security requirements before deployment in telecommunication network.

The Telecom Security Operation Centre (TSOC) has been established to monitor the national telecom infrastructure, identify malicious patterns and to send regular actionable alerts to telecom stakeholders towards enhancement of the cybersecurity posture of the sector.

(b): The Telecommunications Act, 2023 provides for notification of standards and conformity assessment measures for telecommunication equipment, networks and services.

The Telecommunications (Standards, Conformity Assessment and Certification) Rules, 2025 have been notified. These rules empower the Telecommunication Engineering Centre and the National Centre for Communication Security as the appropriate authorities to notify standards and conformity assessment measures, formulate testing procedures and recognise Conformity Assessment Bodies and laboratories for testing. The testing and certification framework requires that the telecom equipment meet the essential security requirements before deployment in telecommunication networks.

In addition, the National Security Directive on Telecommunications Sector requires telecom service providers to procure and deploy only "trusted products" from "trusted sources" in telecommunication networks. A trusted telecom portal has been developed, which maintains list of trusted vendors and trusted components fulfilling supply chain security requirements.

The security standards are developed based on prevailing best international standards suitably adapted to Indian conditions to address telecommunication network security.

(c): Various measures as mentioned at (a) and (b) above have been taken to improve network redundancy, emergency communication systems and infrastructure resilience. The following additional measures have also been taken:

(i) A Standard Operating Procedure for responding to disasters has been issued to strengthen the resilience of telecom infrastructure through measures covering mitigation, preparedness, response and recovery.

(ii) State-level telecom disaster coordination committees have been formed for coordination among the Department of Telecommunications, telecom service providers, State Governments and Disaster Management Authorities.

(iii) A common alerting protocol based integrated alert system and cell broadcast technology solution has been implemented for timely dissemination of location-specific emergency alerts and disaster warnings to mobile users in affected areas.

(iv) Intra-Circle Roaming is activated in areas where mobile networks of telecom service providers is disrupted enabling affected subscribers to connect to other available mobile networks to maintain continuity of telecom services.

(d): Policy framework for national telecom resilience is in place in the form of law and rules as mentioned. The policy provides a comprehensive protection framework for telecommunication network resilience through cyber security and disaster recovery measures, security standards and supply chain security. The authorised entities are under obligation to comply and thereby ensuring uninterrupted, resilient and secure delivery of services.

In addition, the Indian Computer Emergency Response Team (CERT-In) has been established under the Ministry of Electronics and Information Technology as the national nodal agency for responding to cybersecurity incidents under the Information Technology Act, 2000. CERT-In gathers threat intelligence and issues telecom specific alerts and provides cyber incident response support.

The National Critical Information Infrastructure Protection Centre has been established under the aegis of the National Technical Research Organisation, to serve as the national nodal agency for the protection of Critical Information Infrastructure (CII) from cyber threats under the Information Technology Act, 2000. The said Centre has designated critical elements of national telecom infrastructure as protected systems with a view to safeguard them through comprehensive monitoring, analysis, guidance and incident response support.

*****