

Govt. Notifies Telecommunication Cybersecurity Rules Under Telecom Act, 2023

October 27, 2025 • vajiramandravi.com



What's in today's article?

- Why in the News?
- About Telecommunications Act, 2023
- Telecommunication Cybersecurity Rules Under Telecom Act, 2023

Why in the News?

- The Department of Telecommunications (DoT) has published four sets of draft rules under the Indian Telecommunications Act, 2023. One of these includes Cybersecurity Rules.
- These rules mandate specific measures for telecom entities and outline clear obligations to enhance cybersecurity.

About Telecommunications Act, 2023

- Earlier, the Indian Telecommunications sector was governed by three separate Acts of Parliament:

- **Indian Telegraph Act 1885,**
- **Indian Wireless Telegraphy Act 1933,**
- **Telegraph Wires, (Unlawful Protection) Act 1950**
- The Telecommunications Act, 2023 was brought in to consolidate these three separate Acts.
- **Aim:** To amend the existing laws governing the provision, development, expansion and operation of telecommunication services, telecom networks and infrastructure, in addition to assignment of spectrum.

Telecommunication Cybersecurity Rules Under Telecom Act, 2023

• Data Collection and Analysis:

- The government or authorized agencies can request telecom companies for **traffic data** or other data for cybersecurity purposes.
- **Message data** (e.g., text, audio, video) is excluded from the scope of government requests.
- **Traffic data** includes information generated, transmitted, received, or stored in telecommunication networks, such as type, routing, duration, and timing.
- Telecom companies must establish infrastructure to collect traffic data and provide it to the government at designated points for analysis, processing, and sharing with authorized entities.

• Cybersecurity Compliance and Reporting:

- **Cybersecurity Policy:** Telecom companies must adopt and report on a cybersecurity policy that includes:
 - Security safeguards and risk management practices.
 - Procedures for network testing and incident response systems.
 - Forensic analysis measures for cybersecurity incidents.
- **Security Audits:** Companies must conduct periodic cybersecurity audits through government-certified agencies.
- **Security Operations Centre (SOC):** Telecom companies must establish SOCs to monitor and handle cybersecurity incidents.
- **Incident Reporting:**
 - Initial reporting of **cybersecurity** incidents within **6 hours** of awareness.
 - Detailed reports (e.g., number of users affected, geographic impact, remedial actions) within **24 hours**.
- **Compliance Portal:** Companies must furnish cybersecurity compliance reports on a government portal or through secure communication channels.

• Security Incident Response:

- The government may direct telecom companies to:
 - Prevent or remedy cybersecurity incidents within a specified time frame.
 - Disconnect telecom identifiers linked to threat actors.
- Companies must appoint a **Chief Telecommunication Security Officer (CTSO)** to coordinate incident response and compliance
- The government can disclose incident details to the public or require telecom companies to do so.

• Equipment Security Regulations:

- Telecom equipment with an **IMEI number** must be registered with the government.

- It is prohibited to:
 - Alter or remove telecommunication equipment identifiers.
 - Use devices with tampered identifiers to produce traffic.
- The government may block equipment with tampered IMEI numbers or direct manufacturers to assist in addressing such issues.

- **Digital Implementation:**

- A government portal will facilitate the digital implementation of these rules.
- Secure communication mechanisms may be used for issuing orders, collecting information, or reporting compliance.

- **Key Provisions Unchanged from the Original Draft Rules:**

- The government can take action against threat actors by disconnecting identifiers.
- Directions may be issued to telecom companies to prevent or address security incidents.
- Tampering with equipment identifiers remains strictly prohibited.

This structured format ensures clarity in understanding the roles and responsibilities of telecom companies and the government's authority under the Telecommunication Cybersecurity Rules.

Q1. How big is the telecommunication industry in India?

The Telecom industry in India is the second largest in the world with a subscriber base of 1.179 Bn as of August 2023 (wireless + wireline subscribers).

Q2. How do satellite phones work?

A satellite phone has an omnidirectional or directional antenna that is used for both transmitting and receiving signals. In order to receive a signal for service, most satellite phones require a line-of-sight with the sky.

News: Govt notifies telecom cyber security rules, sets reporting timelines | Hindu

Source: <https://vajiramandravi.com/current-affairs/govt-notifies-telecommunication-cybersecurity-rules-under-telecom-act-2023/>

© Vajiram & Ravi. For personal use only.