New Telecommunication Cybersecurity Rules

Posted at: 23/11/2024

Govt. Notifies Telecommunication Cybersecurity Rules Under Telecom Act, 2023

Context : The **Telecommunications Act, 2023** in India introduces a comprehensive framework for regulating the telecom sector and enhancing **cybersecurity** in telecommunications. The Act consolidates previous outdated laws and includes detailed **Cybersecurity Rules** for telecom companies. Below is an **elaborate and clear breakdown** of the key provisions under the **Telecommunication Cybersecurity Rules**.

Background: Telecommunication Laws in India

Before the **Telecommunications Act, 2023**, India had three separate Acts that governed telecommunications:

1. **Indian Telegraph Act, 1885**
2. **Indian Wireless Telegraphy Act, 1933**
3. **Telegraph Wires (Unlawful Protection) Act, 1950**

The new **Telecommunications Act, 2023** was created to **consolidate** and **modernize** these outdated laws. The aim is to improve the regulation of:

- **Telecommunication services**
- **Telecom networks and infrastructure**
- **Spectrum allocation**

This law ensures the **development, operation, and expansion** of telecom services in line with modern technological needs.

Telecommunication Cybersecurity Rules: Key Provisions

1. Data Collection and Analysis

- **Traffic Data**: Telecom companies are required to **collect and store specific data** related to telecommunication traffic. This includes information such as:

    - **Call duration**
    - **Routing**
    - **Timing and type of communication (e.g., voice, video, text)**

- **Exclusion of Message Content**: The rules clarify that **message content** (e.g., text, audio, video) is **excluded** from government requests for data. The government can only ask for **traffic data**, not personal content.

- **Government Access**: Authorized government agencies may request telecom companies to provide traffic data for **cybersecurity analysis**, but only through clearly defined channels.

---

2. Cybersecurity Compliance and Reporting

Telecom companies must implement strong cybersecurity measures and regularly report their efforts:

- **Cybersecurity Policy**: Companies are required to adopt a **comprehensive cybersecurity policy** that should include:
    - **Risk management practices**
    - **Network testing and incident response protocols**
    - **Forensic analysis** for incidents

- **Security Audits**: Companies must conduct **periodic audits** of their cybersecurity systems through **government-certified agencies**.

- **Security Operations Centres (SOC)**: Telecom firms must set up **Security Operations Centres** to continuously monitor and respond to cybersecurity threats.

---

3. Incident Reporting

- **Initial Reporting**: Telecom companies must report any cybersecurity incidents within **6 hours** of becoming aware of them.

- **Detailed Reporting**: Within **24 hours**, companies must submit a **detailed report** to the government, which includes:
    - The **number of affected users**
    - The **geographic impact**
    - The **remedial actions taken** to address the incident

- **Compliance Portal**: Telecom companies must upload all reports to a **government**

compliance portal or share them through **secure communication channels**.

---

4. Incident Response and Government Directives

- **Government Oversight**: The government has the authority to direct telecom companies to take actions such as:
  - **Disconnecting telecom identifiers** (like phone numbers or device IDs) linked to **cybercriminals** or **threat actors**.
  - **Preventing or remedying** cybersecurity incidents within a specified time frame.
- **Appointment of CTSO**: Each telecom company must appoint a **Chief Telecommunication Security Officer (CTSO)**. The CTSO is responsible for:
  - Overseeing the company's cybersecurity efforts
  - Coordinating **incident response**
  - Ensuring compliance with cybersecurity rules
- **Public Disclosure**: In some cases, the government may require telecom companies to **disclose incident details publicly** or disclose them themselves.

---

5. Equipment Security Regulations

- **IMEI Registration**: All telecom equipment with an **IMEI number** (used for device identification) must be **registered with the government**.

- **Prohibition of Tampering**: It is strictly prohibited to:

  - **Alter or remove IMEI numbers** from telecom equipment.
  - Use **tampered devices** to produce traffic or bypass security measures.

- **Blocking Tampered Devices**: The government has the authority to **block devices** with tampered IMEI numbers or instruct manufacturers to assist in addressing such issues.

---

6. Digital Implementation

- **Government Portal**: A **dedicated digital platform** will be used for:

  - **Reporting compliance**
  - **Incident reporting**
  - **Exchanging secure communications** between telecom companies and the government.

- **Secure Communication**: Telecom companies and the government will use **encrypted channels** to share sensitive data and orders.

Key Provisions Remain Unchanged

The final rules have retained several critical provisions from the original draft:

- **Disconnecting Identifiers**: The government can still disconnect telecom identifiers (like phone numbers or device IDs) tied to **cybersecurity threats**.
- **Timely Incident Response**: Telecom companies are still required to act quickly to **prevent or address cybersecurity incidents**.
- **No Tampering with Equipment**: Altering or removing equipment identifiers remains **illegal**.

Conclusion

The **Telecommunication Cybersecurity Rules** under the **Telecommunications Act, 2023** aim to **strengthen cybersecurity** in India's telecom sector. By enforcing **data collection, incident reporting**, and **compliance measures**, the government seeks to protect the country's growing digital infrastructure. Telecom companies must adopt strong cybersecurity policies, conduct regular audits, and implement robust incident response systems to protect against cyber threats. The law establishes a balance between **government oversight** and the need for **secure telecommunications** in a digital-first world.