INDIALAW

CIVIL

Strengthening India's Digital Frontiers: Key Insights into the Telecom Cyber Security Rules 2024

AUTHOR Rahul Sundaram

PUBLISHED 27 November 2024

In a world increasingly reliant on telecommunications, the **Telecommunications (Telecom Cyber Security) Rules, 2024**, emerge as a cornerstone of India's efforts to bolster its digital infrastructure. Issued under the **Telecommunication Act, 2023**, these rules provide a comprehensive framework to secure the nation's telecom networks, protect user data, and ensure robust responses to cyber threats.

Table of contents

A New Legal Foundation

The new rules draw their authority from **Section 22(1)** and **Section 56(2)(v)** of the **Telecommunication Act, 2023**. They replace the outdated **Prevention of Tampering of Mobile Device Equipment Identification Number Rules, 2017**, and the **Mobile Device Equipment Identification Number (Amendment) Rules, 2022**, while retaining the validity of past actions under those regulations.

Key Definitions

Understanding these rules begins with defining critical terms:

- **Telecom Cyber Security** encompasses tools, policies, technologies, and actions designed to safeguard telecom networks, services, and associated data from cyber threats.
- **Telecommunication Entity** refers to providers of telecom services and operators of telecom networks.
- **Chief Telecommunication Security Officer (CTSO)** is a designated official responsible for implementing these rules and ensuring compliance.
- **Security Incident** is any event that potentially disrupts telecom cyber security.

These terms establish the groundwork for precise interpretation and application of the rules.

Core Provisions

1. Data Collection, Sharing, and Analysis

The rules empower the **Central Government** and its authorized agencies to collect **traffic data** and other relevant information to ensure telecom cyber security. Telecom entities may be directed to install infrastructure for seamless data collection and processing. Importantly:

- The data can only be used to enhance telecom cyber security.
- It may be shared with law enforcement agencies or telecom stakeholders if deemed necessary.
- Strict safeguards are mandated to prevent unauthorized access.

2. Obligations on Telecom Entities

The rules place substantial responsibility on telecom entities to:

- **Develop Cyber Security Policies**: Entities must craft policies incorporating risk assessments, network testing, and response strategies for security incidents.
- **Conduct Security Audits**: Both internal and government-certified audits are required.
- **Report Security Incidents**: Entities must notify the government within **six hours** of an incident, detailing its impact and mitigation steps.
- **Establish Security Operations Centres (SOC)**: SOCs will monitor threats, log incidents, and maintain records critical to cyber defence.

3. Measures for Threat Mitigation

The government has introduced a process to identify and respond to cyber threats:

- Upon detecting risks, a **notice** is issued to the individual or entity associated with the threat, requiring a response within seven days.
- Failing a response, or based on findings, the government may suspend or terminate telecom services linked to compromised identifiers.
- Actions may extend to all associated telecom equipment or identifiers.

4. Appointment of Chief Telecommunication Security Officer

Every telecom entity must appoint a **CTSO**, who:

- Must be an Indian citizen and resident.
- Reports directly to the entity's board.
- Acts as the key liaison with the government, ensuring compliance and reporting security incidents.

5. Reporting of Security Incidents

1. **Incident Reporting (Within 6 Hours)**: Telecommunication entities must report any **security incident** affecting them to the Central Government within **6 hours**.
2. **The report must include details such as:**
    - Number of users affected.
    - Duration of the incident.
    - Geographical area impacted.
    - Extent of disruption to telecommunication networks or services.
    - Economic and societal impact.
    - Remedial measures taken or proposed.
3. **Public Disclosure**:
    - The Central Government may disclose the incident to the public if it deems it in the **public interest**, or it may require the affected entity to do so.
4. **Information and Audits**:
    - Affected entities may be directed to:
        - Provide information for assessing the security of networks and services.
        - Conduct a **security audit** by a government-specified certified agency at their own cost.
5. **Government Directives**:
    - The government can issue **remedial measures** or preventative directions to mitigate the incident or avert significant threats.
    - Specific timeframes for compliance may be set for the affected entities.

6. Equipment and Identifier Safeguards

The rules address vulnerabilities in telecom equipment:

- Manufacturers and importers of devices with **International Mobile Equipment Identity (IMEI)** numbers must register them with the government before sale or import.
- Tampering with identifiers or related hardware/software is strictly prohibited.
- The government may order telecom entities to block devices with tampered IMEI numbers.

7. Digital Implementation

Digital tools are at the heart of the rules' execution. These tools facilitate:

- Real-time data collection, analysis, and reporting.
- Digital submission of policies and security reports.
- Maintaining a repository of actions taken against violators.

Conclusion: A Secure Future for Indian Telecom

The **Telecommunications (Telecom Cyber Security) Rules, 2024**, reflect India's commitment to a secure and resilient telecom ecosystem. By introducing rigorous safeguards, ensuring accountability through the CTSO, and leveraging digital tools, these rules address the growing complexity of cyber threats in the telecom sector. As the nation strides forward in its digital journey, these rules serve as a critical pillar, protecting users and strengthening trust in India's telecommunications infrastructure.

For further details write to contact@indialaw.in