KHAITAN &CO ADVOCATES SINCE 1911

UPDATE

ERGO

Analysing developments impacting business

TELECOM CYBER SECURITY RULES: A FRAMEWORK TO BOLSTER SECURITY IN THE TELECOM SECTOR

9 September 2024

Introduction

On 28 August 2024, the Department of Telecommunication (DoT) published the draft Telecommunications (Telecom Cyber Security) Rules, 2024 (Rules) in exercise of the powers conferred under the Telecommunications Act, 2023. The Rules are designed to ensure '*telecom cyber security*', which essentially refers to use of policies and processes to address emerging cyber security threats and ensure the integrity and security of the telecommunication networks, services and infrastructure across India.

These Rules, which will be taken into consideration after expiry of 30 days from the date of publication, impose compliance obligations on 'Telecommunication Entities' i.e., any person or company providing telecommunication services or establishing, operating, maintaining or expanding a telecommunication network and includes licensed telecom service providers (Telecom Entity).

The Rules supersede the erstwhile rules framed under the Indian Telegraph Act, 1885, namely the Prevention of Tampering of the Mobile Device Equipment Identification Number Rules, 2017 which were introduced in 2017 and thereafter amended in 2022 (MDEI Rules).

Key provisions under the Rules:

1. **Power to seek traffic data**: The Rules empower authorised agencies to seek traffic and other data from any Telecom Entity and to direct a Telecom Entity to establish necessary infrastructure and equipment for collection and provision from designated points, coupled with provisions that require such government agencies to prevent unauthorized access or use of this data. Such data collected may be analysed for improving telecom cybersecurity and be shared with relevant government agencies or telecommunication entities or users.
2. **Reporting of security incidents**: Telecom Entities are required to report any 'security incidents' to the Central Government within 6 hours of its occurrence. Importantly, 'security incident' is defined in an extremely wide manner to include any event that has an actual or potential adverse effect on telecom cybersecurity. Such report must include details such as the number of users affected, the duration of the incident, the geographical area affected, the extent of the impact on the network or services and remedial measures taken. The Central Government may also require the disclosure of certain incidents to the public if deemed necessary in the public interest. The Central Government may also require the impacted Telecom Entity to undergo a security audit by a certified agency and implement suggested remedial measures.
3. **Other obligations of Telecom Entities**: Telecom Entities have several obligations under these rules, including:

a *Appointment of Chief Telecommunication Security Officer (CTSO)*: Each Telecom Entity is required to appoint a citizen and resident of India as a CTSO and notify such details to the Central Government. The CTSO is responsible for coordinating with the Central Government to ensure compliance with these Rules including any reporting requirements under the Rules.

b *Adoption of cybersecurity policy*: Telecom Entities must adopt a comprehensive cybersecurity policy that comprises of security safeguards, risk management approaches, and best practices, and consequently put in place measures to enforce such policy.

c *Network testing and risk management*: Entities are required to undertake regular testing of telecommunication networks, including vulnerability assessments and penetration testing, to identify and mitigate risks.

d *Establishment of incident response mechanisms*: Entities must establish rapid action systems to respond to security incidents, mitigate impact of such incidents and conduct forensic analyses to learn from such incidents and further strengthen cyber security.

e *Conducting periodic cyber security audits*: Telecom Entities are required to conduct periodic cyber security audits through its own mechanisms and through government certified agencies to assess resilience to telecom cyber security threats.

4. **Power to suspend / terminate telecom identifier that endangers telecom cyber security:** The Central Government may issue show cause notices to individuals or entities whose telecom identifiers are suspected of being involved in such endangering activities and thereafter order the temporary suspension or termination of the use of such telecom identifiers after following due process.

5. **Obligations relating to Telecommunication Equipment**: Manufacturers and importers of telecommunication equipment with International Mobile Equipment Identity (IMEI) numbers are required to register these numbers with the Central Government before selling or importing the equipment in India. Under the superseded MDEI Rules, manufacturers were required to obtain the right to assign a Mobile Device Equipment Identification Number (MDEI) to a mobile device, however, no such requirement has been set out in the Rules. The Rules further prohibit tampering or alteration of unique telecommunication equipment identification numbers (i.e., a number / signal that uniquely identifies a telecom equipment including an IMEI number or electronic serial number). It is pertinent to note here that the MDEI Rules defined MDEI as unique identification numbers for mobile wireless communication devices, however, the Rules expand this definition as unique numbers for any type of telecommunication equipment.

6. **Digital Implementation and Enforcement**: The Central Government may specify digital means for implementing these Rules (upon taking effect), including for collection, sharing, and analysis of traffic data; issuance of notices and submission of responses; maintaining a repository of individuals and telecommunication identifiers against which actions have been taken; preventing the misuse of telecommunication identifiers or services, etc.

Conclusion

The Rules propose a robust legal framework and by mandating strict cybersecurity policies, incident reporting, and compliance measures, these rules ensure that Telecom Entities are well-prepared to combat cyber threats. While there are similarities with prevailing guidelines and instructions issued by the DoT, the Rules also prescribe certain additional requirements that may lead to additional costs and increase the compliance burden for Telecom Entities. For instance, the obligation requiring Telecom Entities to report actual or potential security incidents within 6 hours of its 'occurrence' (rather than the time from when the incident is noticed) seems highly onerous and cumbersome in comparison to similar requirements under other frameworks. Additionally, the Rules grant the Central Government very wide powers to suspend / terminate any telecom identifier with immediate effect. Nevertheless, the Rules are a welcome step in the overall scheme of things.

- *Harsh Walia (Partner); Abhinav Chandan (Partner); Shobhit Chandra (Counsel) and Khyati Goel (Associate).*

For any queries please contact: editors@khaitanco.com