KHAITAN &CO ADVOCATES SINCE 1911

UPDATE

ERGO

Analysing developments impacting business

TELECOM CYBER SECURITY RULES 2024 FINALIZED: KEY UPDATES AT A GLANCE

29 November 2024

On 21 November 2024, the Department of Telecommunications (DoT) issued the final Telecommunications (Telecom Cyber Security) Rules, 2024 (Rules), replacing the earlier draft released for public consultation on 28 August 2024 (see here for our ERGO on the draft rules). The key changes incorporated in the final Rules are:

1. ***Definition of 'certified agency'***. The Rules introduce the term *'certified agency'*, defined as an agency specified by the Central Government on the designated portal to carry out security audits. This ensures a standardised security audits, enhancing telecom cybersecurity through regulatory oversight.

2. ***Creation of a digital 'portal'***. The Rules establish an online *'portal'* to facilitate digital implementation, enabling the Central Government to issue orders, directions, and other communications. Telecom entities must use this portal to fulfil their reporting and information submission obligations. Introduction of this online portal significantly reduces time and costs associated with administrative paperwork.

3. ***Changes in data collection and analysis rule***. Rule 3 empowers the Central Government or its authorized agencies to request traffic data and other information from telecom entities. The Rules introduce a new limitation, explicitly excluding the *content of messages* from such data requests. Additionally, the Rules specify that collected data can only be used by the Central Government, its authorized agencies, or telecom entities for the purpose of ensuring cyber security. This change balances out the concerns associated with excessive surveillance and data access requests.

4. ***Compliance with directions and standards***. Telecom entities are now required to comply with directions and standards issued under the Rules, including adhering to specified timelines. These measures aim to prevent the misuse of telecom identifiers, equipment, networks, or services and to enhance cyber security across the telecom ecosystem.

5. ***Reporting obligations***. Telecom entities must submit a detailed report outlining the measures implemented to ensure cyber security. The Central Government can now also seek clarifications and issue directions, orders, or instructions to address identified risks.

6. ***Temporary suspension of telecom identifiers***. The Rules allow a person reasonable opportunity of being heard, if the Central Government passes an order to temporarily suspend or permanently disconnect the telecom identifier (i.e., series of digits, characters, etc. used to identify a user, an authorised entity or telecom

service, network or equipment) of such person. For clarity, under the Rules, in circumstances deemed necessary and expedient in the public interest, the suspension can occur without prior notice. While such powers of Central Government may raise concerns about operational disruptions, the recent amendments also ensure fairness and due process in decisions to suspend or disconnect telecom identifiers.

7. ***Reporting security incidents***. The updated rules relax incident reporting requirement to 6 hours of becoming *aware* of an incident (as opposed to 6 hours from *occurrence* of the incident), with only relevant details of the affected system and description of the incident. Additionally, the requirement to furnishing additional information relating to the incident may be undertaken within 24 hours of becoming *aware* of such incident.

Comments

The Rules mark a significant shift in the telecom cybersecurity landscape, emphasizing robust compliance and cyber resilience. By introducing mandatory reporting, defining certified audit agencies, establishing a centralized digital portal, and ensuring fairness through procedural safeguards, these rules seek to balance out cybersecurity needs with the risk of arbitrary actions. The role of the Security Operations Centre has also been expanded to monitor attempts to cause telecom cyber security and security incidents, intrusions or breaches. While these measures bring increased compliance costs and obligations for telecom entities, they also work towards building a secure and trustworthy digital ecosystem which is crucial for India's growing digital economy.

- *Harsh Walia (Partner); Sanjuktha A Yermal (Senior Associate) and Vanshika Lal (Associate)*

For any queries please contact: editors@khaitanco.com