KHAITAN &CO ADVOCATES SINCE 1911

UPDATE

ERGO

Analysing developments impacting business

A NEW ERA FOR TELECOMMUNICATION INFRASTRUCTURE: DoT Releases New Rules for Critical Telecommunication Infrastructure

12 September 2024

On 28 August 2024, the Department of Telecommunications (DoT) released the draft Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024 (Rules) for governing 'critical telecommunication infrastructure' (CTI). The Rules are slated to be taken into consideration after expiry of 30 days from the date of its publication in the Official Gazette. In the meantime, stakeholders can submit observations and suggestions in respect of the Rules.

The Rules aim to establish a framework for the management and oversight of CTI. This includes defining CTI, setting out compliance requirements, and outlining the responsibilities of 'telecommunication entities' i.e., entities that provide telecom services and establish, operate, maintain and expand telecom networks, including entities that are authorised or exempted under the Telecom Act (Telecom Entity).

Key provisions of the Rules:

- *Classification of CTI.* The Rules provide that the Government may classify certain telecom infrastructure as CTI based on an assessment of whether disruption of such infrastructure will have a debilitating impact on national security, economy, public health or safety of the nation. For the purposes of enabling such notification, the Government will seek details of telecommunication network, telecommunication services, elements of network, etc. from Telecom Entities.

- *Compliance Requirements.* Telecom Entities will be required to adhere to specific security standards, specifications, interface requirements, etc. issued by the Government for CTI. This includes conformance to requirements and standards stipulated by the Telecommunication Engineering Centre, National Centre for Communications Security, etc. as well as the National Security Directive on Telecommunication Sector.

- *Power to Inspect CTI.* The Government will have the authority to inspect CTI to ensure compliance with the Rules.

- *Chief Telecommunication Security Officer.* Each Telecom Entity will be required to appoint a Chief Telecommunication Security Officer (CTSO) (appointed pursuant to the Telecommunications (Telecom Cyber Security) Rules, 2024 (Cybersecurity Rules)) who will be the point of contact to the Government for implementation of the Rules. The CTSO will be responsible for providing the details of (a) logs for real time monitoring by the Government, (b) service level agreements pertaining to CTI, (c) cyber-crisis management plan for CTI, etc.

- *Obligations of Telecom Entities*. The Rules prescribe various obligations in relation to CTI. Some of the notable obligations are:
    - Compliance with to be prescribed standards, upgradation requirements, etc. for CTI.
    - Maintenance of a complete list of Critical Telecommunication Infrastructure along with the software and hardware details including details of architecture and any changes in such architecture.
    - Development and maintenance of adequate verification practices and protocols applicable for all personnel authorised to have access to CTI.
    - Maintenance of records of the supply chain of the telecommunication equipment and other equipment deployed in CTI till such CTI is in use.
    - Ensuring that remote access to CTI for the purpose of repair or maintenance and production of such logs to the government, if required.
    - Implementation of standard operating procedures for security incident response systems and mechanisms to ensure intimation of security incidents to the Government within 2 hours of occurrence of such incidents.
- *Intimation of Security Incidents*. The Rules provide that any security incident (as defined under the Cybersecurity Rules) in relation to CTI will have to be intimated to the government within two hours of occurrence of such incident.
- *Prior Approval and Certification for Upgradation*. Upgradation to equipment which form a part of the CTI will require prior written approval from the government.

Comments

During the COVID-19 era, telecommunications was designated as an 'essential service' under the Disaster Management Act, 2005. The new Rules aim to provide greater specificity by introducing the concept of CTI as a different class of telecom infrastructure. Additional and stricter regulations surrounding CTI (compared to existing regulatory and license conditions), including shorter reporting timelines for security incidents compared to those under the Unified License or the Cybersecurity Rules, and the requirement to appoint a CTSO, reflect the Government's effort to ensure the robust protection of CTI and align with international standards. Additional compliances include extended timelines for preservation of logs and mandatory written approvals from the Government for upgrading CTI. This will be a key lookout area for stakeholders.

In combination with the Cybersecurity Rules, the Rules may provide to be an effective response to the increasing importance of and reliance on telecommunications infrastructure, as well as prevailing threats. However, considering that the assessment criteria is rather wide, it will be interesting to see how the classification of CTI takes place once the Rules are brought into effect, including for entities such as Infrastructure Provider – Category I entities which are currently non-licensed entities but may be subject to the 'authorization framework' under the Telecom Act going ahead.

- *Harsh Walia (Partner); Abhinav Chandan (Partner); Shobhit Chandra (Counsel) and Vanshika Lal (Associate)*

For any queries please contact: editors@khaitanco.com