Summary: Submission on the draft Telecommunication Rules, 2024

The Data Security Council of India (DSCI) submitted detailed inputs to the Department of Telecommunications (DoT) on the Draft Telecommunication Rules, 2024, with a focus on strengthening cybersecurity in the telecom sector while promoting innovation, regulatory clarity, and ease of doing business.

The submissions appreciated the government's proactive approach to securing the telecom ecosystem—an essential enabler of India's digital economy. While welcoming the draft rules, DSCI emphasized the importance of ensuring that new regulatory obligations are proportionate, risk-based, and harmonized with existing frameworks, particularly for small and medium enterprises (SMEs) and emerging technology providers.

Some of the key recommendations included:

1. **Clarity in Definitions and Scope**

DSCI recommended that the term "telecommunication entity" be clearly defined to avoid ambiguity and overregulation, especially for players like M2M providers, IP-1s, and OSPs that may not have direct security responsibilities.

2. **Need for harmonised cyber security frameworks**

Highlighting the growing overlap among multiple regulatory instruments (DoT, MeitY, CERT-In, NCIIPC), DSCI called for harmonized cybersecurity requirements across sectors to reduce compliance burden, avoid duplication, and support proactive risk management.

3. **Advocacy for a risk-based regulation of the telecom sector regulation**

DSCI advocated for differentiated compliance obligations based on risk profiles, size, and role within the telecom ecosystem. A tiered model would ensure that smaller players can meet compliance expectations without stifling innovation.

4. **Assessing the need for inter-regulatory coordination**

Given the intersection of telecom, cybersecurity, and critical infrastructure, DSCI recommended the development of a coordinated inter-regulatory framework. This would include clarity on roles across ministries, standardized reporting templates, and regular inter-agency coordination.

5. **Ensuring Operational Flexibility**

The submission flagged concerns around duplicative roles—such as the requirement for a Chief Telecom Security Officer (CTSO) despite the existing mandate for Chief Information Security Officers (CISOs). DSCI proposed aligning and enhancing existing roles instead of introducing new ones.

6. Practical Compliance Measures

Key implementation-related suggestions included:

- Relaxing the strict six-hour security incident reporting window to allow more complete and accurate submissions.
- Replacing prior-approval requirements for infrastructure upgrades with periodic post-facto reporting.
- Avoiding overly broad definitions of "traffic data" and ensuring privacy safeguards are built in line with the Digital Personal Data Protection Act, 2023.
- Introducing more objective and transparent criteria for classifying Critical Telecommunication Infrastructure (CTI).
- Encouraging a risk-based, context-specific approach to internet suspension orders to minimize socio-economic disruptions.

Conclusion

DSCI's recommendations are aimed at creating a secure, resilient, and innovation-friendly telecom environment. By advocating for a proportionate and harmonized regulatory framework, DSCI seeks to support India's ambition of becoming a global digital and telecom hub while ensuring the security and privacy of its digital infrastructure.