

DSCI's Submission on Draft Telecom Cybersecurity Rules, 2025

Our submission broadly supports the intent of the draft rules but underscores the importance of ensuring that the framework remains proportionate, practical, and innovation friendly. Several key aspects require further deliberation:

1. Scope & Applicability: The draft rules extend beyond telecom licensees and service providers to cover entities such as fintech platforms, e-commerce players, and OTT providers. Such an expansion risks going beyond the mandate of the Telecommunications Act, 2023, potentially leading to duplication of obligations and regulatory overreach.

2. Jurisdictional Clarity: There are overlaps with existing legislations such as the IT Act, 2000, the DPDP Act, 2023, and sectoral regulations issued by RBI, SEBI, IRDAI, and TRAI. Without alignment, these overlaps may create operational uncertainty and increase compliance costs. A clear demarcation of jurisdiction between DoT and MeitY is essential.

3. Compliance & Operational Challenges: Some provisions, such as mandatory Mobile Number Validation (MNV), while well-intentioned, may impose significant costs and operational complexity on startups, MSMEs, and smaller entities. Unless carefully calibrated, these requirements may risk stifling innovation and ease of doing business.

4. Mobile Number Validation (MNV) Platform: The framework for MNV needs stronger safeguards. Concerns include proportionality of data collection, privacy implications, legality of mandate, and long-term sustainability. Any such mechanism must include robust checks on data handling, clear purpose limitation, and accountability mechanisms.

5. Government Data Access: The rules envisage government access to telecom identifier data for cybersecurity purposes. While national security is paramount, such access must be balanced with safeguards defining the scope, ensuring necessity and proportionality, and instituting procedural checks to maintain citizen trust.

Recommendations: We recommend that the DoT adopt a risk-based and consultative approach that:

- Limits obligations strictly to telecom service providers,
- Harmonizes with existing laws and regulatory frameworks,
- Embeds privacy and proportionality as core principles, and
- Ensures compliance mechanisms are feasible, cost-effective, and innovation-enabling.

A framework built on clarity, proportionality, and collaboration will enable the telecom sector to meet cybersecurity goals without undermining India's broader digital transformation and innovation ecosystem.