ACT Association for Competitive Technology

27 November 2026

Shri Akhilesh Kumar Trivedi
Advisor (Networks, Spectrum and Licensing)
Telecom Regulatory Authority of India
World Trade Centre, Tower F, Nauroji Nagar
New Delhi 110029, India
By email: advmn@trai.gov.in

Re: Comments of the Association for Competitive Technology (ACT) on the Draft Guidelines on Responsible Use of Artificial Intelligence (AI) in Telecommunication Networks and Provision of Telecommunication Services

Dear Shri Trivedi,

The Association for Competitive Technology (ACT) welcomes the opportunity to comment on the Telecom Regulatory Authority of India's (TRAI) Draft Guidelines on Responsible Use of Artificial Intelligence (AI) in Telecommunication Networks and Provision of Telecommunication Services (the Draft Guidelines), released on 30 October 2026.[1]

ACT is a not-for-profit global trade association representing startups, scaleups, and small and medium-sized technology companies, and it works with policymakers around the world to support an environment in which technology businesses can grow, compete, and succeed. ACT also provides its members with advocacy, insights, and resources to help them scale, raise capital, and compete in global markets.[2] Our members build software, apps, connected devices, and AI-enabled tools used by consumers and enterprises in India and around the world, and many of them sell products and services to telecommunications operators or offer services that run over their networks.

The Draft Guidelines apply directly only to applicable authorised entities, but their due diligence, disclosure, and contracting requirements will determine what those entities ask of the companies that supply them with AI systems. Accordingly, ACT's comments address consistency with India's national approach to AI governance, proportionate treatment of lower-risk AI systems, the obligations that will pass to suppliers, recognition of international standards, and incident reporting.

---

[1] Telecom Regulatory Authority of India, *Draft Guidelines on Responsible Use of Artificial Intelligence (AI) in Telecommunication Networks and Provision of Telecommunication Services* (30 October 2026), https://trai.gov.in/sites/default/files/2026-10/Draft_CP_30102026.pdf.
[2] Association for Competitive Technology, https://actonline.org/.

I. ALIGNING THE GUIDELINES WITH INDIA'S NATIONAL APPROACH TO AI GOVERNANCE

Section 1.1 of the Draft Guidelines states that they build on the India AI Governance Guidelines and are meant to implement them consistently in the telecommunications sector. In releasing the national guidelines, the Ministry of Electronics and Information Technology (MeitY) explained that its focus is on using existing legislation wherever possible,[3] an approach ACT shares. While AI may introduce novel risks in certain contexts, it is a general-purpose technology, and most of the risks the Draft Guidelines identify, such as unintended outcomes that affect service quality, misuse of data, and adversarial attacks on network infrastructure, are already covered by licence conditions, quality-of-service regulations, the Digital Personal Data Protection Act, 2023,[4] and the Telecommunications (Telecom Cyber Security) Rules, 2024.[5] Those Rules already require each telecommunication entity to adopt a telecom cyber security policy, carry out risk assessments and periodic audits, appoint a Chief Telecommunication Security Officer, and report security incidents to the Central Government.

Consistent with the India AI Governance Guidelines' principle of "Innovation over Restraint,"[6] ACT urges TRAI to limit any additional AI-specific obligations to cases where identifiable regulatory gaps exist and where existing technology-neutral requirements cannot adequately address the relevant risks.

ACT asks TRAI to issue the final guidelines as guidance framed around the outcomes it seeks, and to let applicable authorised entities meet those outcomes through their existing governance, risk management, and reporting structures wherever those structures already cover AI systems. An entity should be able, for example, to give the functions of the AI Governance and Safety Committee in section 3.6 to an existing risk or security committee, and to incorporate its internal AI policy under section 3.2 into its telecom cyber security policy, so long as the substance is addressed. That flexibility avoids parallel compliance programmes that add cost without adding protection, and it keeps the telecommunications sector in step with the approach the Government has taken across the economy.

II. PROPORTIONATE TREATMENT OF LOWER-RISK AI SYSTEMS

The Draft Guidelines define an "AI system" broadly, as a machine-based system that infers from its inputs how to generate outputs such as predictions, content, recommendations, or decisions, and they apply to every authorised entity that uses or intends to use such a system. That definition reaches spam and fraud filters, customer-service chatbots, network traffic optimisation, predictive

---

[3] Press Information Bureau, *India's AI Governance Framework to Focus on Human-Centric Development, Responsible AI, and Mitigation of Potential Harms: Shri S Krishnan, Secretary MeitY* (5 November 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2186639.

[4] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023).

[5] Telecommunications (Telecom Cyber Security) Rules, 2024, notified by the Department of Telecommunications on 21 November 2024 under the Telecommunications Act, 2023 (No. 44 of 2023).

[6] Press Information Bureau, *India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation* (15 February 2026), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2026/feb/doc2026215790801.pdf.

maintenance tools, and the AI features now built into ordinary commercial software and devices. Section 3.2(a) sensibly requires entities to classify each AI system as high-, medium-, or low-risk, yet several of the most demanding requirements apply to every AI system whatever its classification. Under section 3.2(b), any AI system may be used only after approval by a designated officer; section 3.5(a) bars the use of any AI system that is not in the inventory; and section 3.5(c) requires validation, conformity assessment, and impact assessment before any new or modified AI system is deployed.

ACT asks TRAI to tie these requirements to the risk classification that the Draft Guidelines already create. Full validation, conformity assessment, and impact assessment should apply to high-risk systems, with a lighter, documented self-assessment for medium-risk systems and a simple record for low-risk systems. Entities should be able to record low-risk systems in the inventory by category, and AI features embedded in general-purpose commercial software, services, or devices that play no part in network operation or in decisions affecting consumers should fall outside the inventory, approval, and assessment requirements. The same reasoning applies to explainability, which section 3.5(c) lists as an element of conformity assessment. How much explanation is technically possible and useful depends on the model and its use, so TRAI should confirm that entities may meet this element through system-level documentation of a model's purpose, inputs, and known limitations, keeping output-level explanation for high-risk uses that directly affect consumers. TRAI should likewise confirm that the human oversight element of section 3.5(c) may be met through monitoring and exception-based intervention for automated network functions that operate in real time, where review of each output is not practical. We also ask that the requirement in section 3.4 to file the internal AI policy with TRAI within seven working days of any amendment apply only to material amendments. Finally, we ask TRAI to allow at least 12 months for entities to build their inventories, review AI systems already in use, and update existing supplier contracts, with new high-risk deployments covered from the date the guidelines take effect.

These changes would also lighten the load on suppliers, because every requirement that attaches to an AI system turns into a request for documentation, test evidence, and contractual commitments from the company that built it. A risk-based approach on the operator side keeps what small suppliers must provide in line with the actual risk of the product they sell.

III. SUPPLIER DUE DILIGENCE, DISCLOSURES, AND CONTRACT TERMS

Sections 3.5(b), 3.5(e), and 3.5(f) require applicable authorised entities to assess supplier credibility, system soundness and limitations, and "the suitability and quality of data used for training"; to obtain AI disclosures from suppliers when procuring equipment, systems, or solutions with embedded AI; and to include in supplier agreements enforceable provisions on regulatory compliance, audit and inspection rights, incident management, risk allocation, and accountability. Section 3.8 makes each entity accountable for the outcomes of every AI system it uses, whether developed in-house, procured, or outsourced. ACT understands TRAI's interest in holding licensees responsible for their networks and services. In practice, however, each operator will write its own questionnaires and contract terms to meet these obligations, and a small developer that sells the same product to several operators could face a different set of disclosure demands, audit clauses, and liability terms from each of them. Many small companies lack the legal and compliance staff to negotiate those terms, and some may conclude that supplying Indian operators is not worth the cost, leaving operators with fewer suppliers to choose from.

ACT therefore asks TRAI to:

1. Ensure that the depth of due diligence under section 3.5(b) and the contractual provisions required by section 3.5(f) scale with the risk classification of the AI system and its intended use, so that a low-risk tool does not carry the same audit and inspection terms as a system that controls core network functions.
2. Confirm that the assessment of training data under section 3.5(b) and the disclosures under section 3.5(e) can be satisfied through summary documentation, such as model or system cards describing the categories and sources of training data, intended uses, performance testing, and known limitations. Training datasets, model weights, and source code are often a small developer's most valuable intellectual property and trade secrets, and requiring their disclosure to each customer would put that property at risk without improving an operator's ability to manage the risks of the system as deployed. The final guidelines should also provide that information a supplier discloses is to be kept confidential and used only for compliance purposes.
3. Confirm that audit and inspection rights can be met through independent certifications and third-party attestations, such as certification of an AI management system under ISO/IEC 42001, together with documentation the supplier provides, in place of on-site inspection of the supplier's facilities and systems. For general-purpose software and cloud services sold to many customers on standard terms, the supplier's standard documentation and certifications should be sufficient.
4. Ensure that the final guidelines state that supplier agreements may allocate responsibility according to each party's role and control. The supplier controls how a system is designed and trained, while the operator controls how it is configured and deployed, what data it receives, and how people oversee it, and responsibility for a given risk should rest with the party best placed to prevent or reduce it. Without such a statement, the accountability rule in section 3.8 is likely to lead operators to demand open-ended indemnities from suppliers for harms that arise from the operator's own deployment choices, which small suppliers cannot absorb.

IV. RECOGNISING INTERNATIONAL STANDARDS

ACT supports the flexibility in section 3.5(c), which permits fairness assessments under TEC Standard 57050:2023 or an applicable international standard, and in section 3.5(g), which permits incident recording under TEC Standard 57090:2025 or an equivalent taxonomy. We ask TRAI to build on this by naming, in the final guidelines or in accompanying guidance, international standards and frameworks that applicable authorised entities and their suppliers may rely on, including ISO/IEC 42001:2023 on AI management systems,[7] ISO/IEC 23894:2023 on AI risk management,[8] and the NIST AI Risk Management Framework.[9] Many ACT members sell into India and other markets at the same time and organise their AI governance around these frameworks. If TRAI confirms that conformity assessments, documentation, and certifications prepared under them can satisfy the corresponding requirements of the guidelines, suppliers will not need to repeat the same work for Indian operators, and operators will have a reliable basis for their due diligence.

[7] ISO/IEC 42001:2023, *Information technology: Artificial intelligence: Management system*.
[8] ISO/IEC 23894:2023, *Information technology: Artificial intelligence: Guidance on risk management*.
[9] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1 (26 January 2023), https://doi.org/10.6028/NIST.AI.100-1.

V. INCIDENT REPORTING

Sections 3.2(d) and 3.9 require critical- and high-severity AI incidents to be reported to TRAI in a form, manner, and timeframe that the Draft Guidelines leave to be prescribed. Telecommunication entities already report security incidents to the Central Government within six hours of becoming aware of them under the Telecom Cyber Security Rules,[10] and report cyber incidents to CERT-In under its directions of 28 April 2022,[11] so an AI incident that affects network security could trigger three separate reports on different timelines. ACT asks TRAI to consult stakeholders before prescribing the form and timeframe for AI incident reports, to align them with the existing regimes so that one report can serve all three where the facts overlap, and to run the reporting clock from when an entity becomes aware of an incident, allowing enough time to confirm that it has occurred and to assess its severity before reporting. Operators will pass these timelines on to their suppliers through the incident management provisions required by section 3.5(f), so the timeframe TRAI chooses will also set what small suppliers must commit to in their contracts.

VI. CONCLUSION

ACT appreciates TRAI's work on the responsible use of AI in telecommunication networks and services and would welcome the opportunity to discuss these comments further.

Sincerely,



Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Global Policy Counsel

Kedharnath Sankararaman
Policy Counsel

Association for Competitive Technology
1401 K St NW (Ste 501)
Washington, DC 20005
United States

[10] Telecommunications (Telecom Cyber Security) Rules, 2024, *supra* note 5.

[11] Indian Computer Emergency Response Team (CERT-In), *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet* (28 April 2022).