Internet And Mobile Association Of India

IAMAI Submission on Consultation Paper on The Terms and Conditions of Network Authorisations to be Granted Under the Telecommunications Act, 2023

Established in 2004, the Internet and Mobile Association of India (IAMAI) is a not-for-profit industry body representing the digital services industry with over 600 Indian and multinational corporations as its members, which include established companies in diverse sectors of the digital ecosystem as well as start-ups. We firmly believe that India's digital industry is going to be a major driving force in the economic and social development of the country which includes job creation, innovation, contribution to the GDP, inclusion and empowerment of our citizens.

On 22 October 2024, Telecom Regulatory Authority of India (TRAI) published the 'Consultation Paper on The Terms and Conditions of Network Authorisations to be Granted Under the Telecommunications Act, 2023'. At the outset, we would like to thank the TRAI for the opportunity to submit our comments on the consultation paper. On behalf of our members, we would like to put forth the following submission. Before we begin, we note that member Reliance Jio has divergent views from those expressed in this document. We also note that our member Airtel has a divergent view from the majority of points raised in this submission.

IAMAI Submission

Q1. Whether there is a need to merge the scopes of the extant Infrastructure Provider-I (IP-I) and Digital Connectivity Infrastructure Provider (DCIP) authorization (as recommended by TRAI in August 2023), into a single authorisation under Section 3(1)(b) of the Telecommunications Act, 2023? Kindly provide a detailed response with justifications.

AND

Q3(b). In case your response to the Q1 is in the negative, whether there is a need to make certain changes in the eligibility conditions, area of operation, validity period of authorisation, scope, and terms & conditions (general, technical, operational, security etc.) of the DCIP authorisation (as recommended by TRAI in August 2023)? If yes, kindly provide a detailed response with justifications

The scope of the proposed authorisation for Digital Connectivity Infrastructure Providers (DCIP) and Infrastructure Provider-1 (IP-1) registration should be merged and expanded further to meet the practical needs of data centres and cloud service providers (CSPs).

Expanding the DCIP authorisation to enable data centres and CSPs to have direct operational control over network infrastructure will enhance the resilience and efficiency of provision of cloud-based services, which will play a central role in advancing India's digital transformation goals.

The Indian data centre industry is experiencing rapid expansion, owing to a fast-growing internet userbase, upward spike in data consumption, and the establishment of a favourable environment for a data economy through the government's Digital India initiative. India is now the home to more than 80 third-party data centres, attracting investments from both local and international stakeholders. The Indian data centre sector is projected to grow at a Compound Annual Growth Rate (CAGR) of 50%

until 2030[1], with emerging trends and technologies fuelling this expansion. The government's Digital India programme, which began in 2015, has moved digitalisation to the forefront, and the National Digital Communications Policy, 2018 (NDCP)[2] emphasises that digital infrastructure and services are increasingly emerging as key enablers and critical determinants of a country's growth and well-being.

The Indian government has also shown a strong commitment to positioning the country as a global data centre hub, in recognising the importance of robust digital infrastructure in driving economic growth, technological advancement, and digital inclusion. The Ministry of Electronics & Information Technology (MeitY), in its 'Draft Data Centre Policy' in 2020[3], set out a comprehensive framework for fostering the data centre sector, including regulatory and structural interventions, investment promotion, and incentivisation mechanisms. The NDCP, and the Propel India mission thereunder, similarly underscores the significance of digital infrastructure. The NDCP, in particular, identifies facilitating the establishment of captive fibre networks by CSPs as a priority objective. This clearly highlights a regulatory focus on equipping the data centre industry with control over establishment and operation of infrastructure that supports efficient, high-speed data transmission. TRAI as well has acknowledged the critical role of data centres in bolstering the data economy, in its Recommendations on 'Regulatory frameworks for promoting data economy through establishment of Data Centres, Content Delivery Networks and interconnect exchanges in India' in December 2021.[4] These policy initiatives indicate the government's alignment on removal of regulatory obstacles to facilitate the growth of India's data economy and create a favourable environment for large-scale data centre operations.

Keeping the above objective in mind, TRAI had proposed the creation of DCIPs as a separate light-touch authorisation under the Unified License. Such authorisation is intended to have no applicable license fee or bank guarantees, specific exemptions from onerous and generic conditions in the Unified License, and a cap on entry fee and application processing fee at INR 2 lakhs and INR 15,000 respectively. The scope of DCIP service is intended to be a national-level, non-exclusive authorisation to own, establish and work (i) all equipment and systems required for establishing WAN, RAN, Wi-Fi systems and transmission links; and (ii) right of way, duct space, dark fibre, poles, tower, feeder cable, antenna, base station, in building solution, distributed antenna system etc. While we are in support of such conditions, we would prefer an expansion of the scope of the authorisation keeping in mind the government's objectives in relation to proliferation of digital infrastructure for data centre industry as outlined above.

The DCIP authorisation aims to extend the range of digital connectivity infrastructure (DCI) that can be owned, established, and provided by DCIPs to encompass both passive and active infrastructure. However, the proposed authorisation falls short of addressing the specific requirements of data centres and CSPs. It allows (i) DCIPs to provide DCI equipment, items, and systems to other telecom service providers (TSPs) and notified entities only, but not other DCIPs or unlicensed entities thereby

[1] https://theprint.in/economy/indias-data-centre-capacity-set-to-see-12x-increase-by-2030-will-benefit-power-companies-too/2139658/; *Is India Building Enough to power its Digital Transformation*, Cushman & Wakefield report dated 27 June 2024, accessible at <https://www.cushmanwakefield.com/en/india/insights/is-india-building-enough-to-power-its-digital-transformation>

[2] https://www.meity.gov.in/writereaddata/files/National_Digital_Communications_Policy%E2%80%932018.pdf

[3] https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf

[4] TRAI Recommendations dated 18 November 2022, accessible at <https://trai.gov.in/sites/default/files/Recommendations_18112022.pdf>

precluding captive use; and (ii) despite its expansive approach, the DCIP authorisation explicitly excludes the provisioning of end-to-end bandwidth by DCIPs using transmission systems.

Even the IP-I authorisation does not permit unlicensed entities to establish and operate passive infrastructure for their own dedicated use. Therefore, even if a data centre or a CSP registers under the IP-1 category, it cannot utilise dark fibre to create point-to-point connections between its own facilities. Consequently, data centres and CSPs will be unable to leverage DCIP or IP-I authorisations to independently establish and activate networks tailored to their service demands, forcing them to rely on licensed TSPs for critical connectivity needs.

Moreover, the limited scope of the proposed DCIP authorisation risks creating bottlenecks for data centres and CSPs seeking to deploy cloud-based services efficiently. These entities require substantial, dedicated network resources that meet their high standards for latency, reliability, and bandwidth, especially as they cater to data-intensive operations across the country. The current regulatory framework, which mandates reliance on third-party TSPs, is likely to impede these service levels and, by extension, stifle the development of the nascent data sector industry and consequently, India's burgeoning data economy.

Data centre operators are not permitted to establish dark fibre and own optical equipment to construct, operate, and manage their own transmission networks tailored to their specific requirements and optimised for customer needs. Reliance on TSPs for connectivity results in issues, as traditional networks operated by TSPs are primarily designed for voice or public data services and are not optimally suited for cloud services. Cloud services demand high availability, bandwidth, and low latency for the transmission of large volumes of data. Consequently, the dependence of data centres and CSPs significantly impedes the efficient provision of cloud-based services.

The necessity for data centres to have control over their interconnectivity is paramount for the growth and efficiency of cloud-based services in India. High-quality telecom connectivity is a critical requirement for data centre operations, as they run applications that need 24x7 uninterrupted connectivity to store and distribute data. This underscores the need for entities like data centre operators to be allowed to construct, operate, and efficiently manage their own captive optical transmission networks. Such control would enable data centres in India to use captive optical transmission networks for better network performance[5], including avoiding latency, accessing greater bandwidth, and ensuring improved stability and security.

IAMAI Recommendation

A single light-touch authorisation framework under the Telecommunications Act 2023 (Act) that facilitates infrastructure sharing with end-users is necessary. Multiple authorisation frameworks for digital infrastructure poses the risk of duplicity of compliances. Likewise, DCIP authorisation should also not be brought under the unified license (UL) framework. As infrastructure providers only provide assets on lease/ rent out/ sale basis; they are not providing services as mentioned in Guidelines for Unified License.

[5] Data centres, 5G push powering fibre cable boom, The Economic Times (3 November 2024), accessible at <https://economictimes.indiatimes.com/industry/telecom/telecom-news/more-than-just-optics-data-centres-5g-push-powering-fibre-cable-boom/articleshow/114891840.cms?from=mdr>

The proposed scope of the merged DCIP and IP-1 authorisation should be revised and expanded. Specifically, we propose that the authorisation should permit (i) provision of services to data centres and CSPs and/ or (ii) authorised entities to establish and light dark fibre for enabling high-speed connectivity for captive use, thereby ensuring operational control of CSPs/ data centres over such captive networks. This would enable data centre operators and CSPs to construct, operate, and efficiently manage their own networks, as configured and optimised to meet customer requirements without being entirely dependent on licensed TSPs for connectivity. More resilient and efficient delivery of cloud-based services is critical to India's digital goals. Moreover, such changes would align with the objectives outlined in the NDCP, which emphasises the key role of digital infrastructure and services in driving a country's growth and well-being. By enabling the establishment of captive fibre networks and promoting the proliferation of cloud-based systems, this would foster the development of India as a global hub for cloud computing, content hosting and delivery, and data communication systems and services.

Q4. (a) Which telecommunication equipment/ elements should be included in the ambit of 'in-building solution' (IBS)?

(b) Whether there is a need to introduce a new authorisation under Section 3(1)(b) of the Telecommunications Act, 2023 for establishing, operating, maintaining or expanding in-building solution (IBS) by any property manager within the limits of a single building, compound or estate controlled, owned, or managed by it? If yes, what should be the eligibility conditions, area of operation, validity period of authorisation, scope, and terms & conditions (general, technical, operational, security etc.) of such an authorisation? Please provide a detailed response with justifications.

Data centre campus infrastructure should be classified as an 'in-building solution' when it involves fibre and equipment serving as a dedicated network within the campus. This aligns with Multiple Operator Fiber Network (MOFN) principles and warrants simplified authorisation rather than complete telecom licensing.

A campus should be defined as a collection of buildings under common ownership and development as a single project. The authorisation should extend for 15 years, matching standard IRU (Indefeasible Right of Use) terms. The technical scope covers fibre and equipment connecting buildings within the same campus for a customer's dedicated use, explicitly excluding enterprise resale.

Q5. Whether there is a need to make any changes in the eligibility conditions, area of operation, validity period of authorisation, scope, and terms & conditions (general, technical, operational, security etc.) of the Content Delivery Network (CDN) authorisation, as recommended by TRAI on 18.11.2022? If yes, what changes should be made in the eligibility conditions, area of operation, validity period of authorisation, scope, and terms & conditions (general, technical, operational, security etc.) of the CDN authorisation? Kindly provide a detailed response with justification.

AND

Q26. Whether there is a need to change/ modify any of the financial conditions of the IXP and CDN authorisations from those recommended by TRAI on 18.11.2022? If yes, please provide a detailed response with justification(s).

CDNs should be completely kept outside the scope of authorisations or any form of registration as CDNs are fundamentally different from telecommunication providers.

CDNs require appliances for computing and storage, and connectivity. Depending on whether they build their own connectivity or not, CDNs are either a customer of telecommunications providers (for internet access) or a private network interconnecting with telecommunications providers (through transit and peering). As CDNs are not telecommunications providers, they should not be regulated as telecommunications providers or subject to any licensing requirements.

CDNs do not require a license to operate in other countries and TRAI should not set this precedent. Conditioning internet interconnection (peering) to an authorisation or registration should not be introduced as it goes against the commonly accepted and global practice of unregulated peering. The internet has thrived, including in India, under an "innovation without permission" approach and efficient, localised exchange of traffic through the growth of CDNs. Introducing a mandatory registration regime would stifle this virtuous circle. Introducing a registration process will also cause delays in both launching new services and expanding existing ones, thereby adversely impacting the ability of CDN providers to respond to evolving market needs.

Also, CDNs contribute to the development of the internet by improving performance, enhancing the ability to handle traffic loads and reduced bandwidth, load balancing and security. In the 2022 TRAI Consultation Paper on the 'Regulatory Framework for Promoting Data Economy through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India', TRAI recognised that India's CDN market will witness a growth of over 700 % between 2018 – 2027 (i.e., from USD 435.2 million in the year 2018 to USD 2846.8 million by 2027).

Lastly, the CDN market is competitive. Many companies offer commercial CDN services: some of them have been established for decades while others are relatively newer companies. Some companies have successfully implemented their own CDN solutions. Evidence of high competition is that the prices for CDN services are constantly dropping. In the absence of any market failure, TRAI should not stifle CDN growth in India by introducing excessive regulations and barriers to entry.

Q9. Whether there is a need to introduce an authorisation under Section 3(1) of the Telecommunications Act, 2023 for establishing, operating, maintaining or expanding ground stations, which may be used to provide ground station as a service (GSaaS)? If yes, what should be the eligibility conditions, area of operation, validity period of authorisation, scope, and terms & conditions (general, technical, operational, security etc.) for the authorisation to establish, operate, maintain, or expand ground stations, which may be used to provide GSaaS? Kindly provide a detailed response with justifications.

Some companies provide Ground Station as a managed service that lets customers control satellite communications, downlink and process satellite data, scale their satellite operations quickly, easily, and cost-effectively, without having to worry about building or managing their own ground station infrastructure. It is pertinent to note that these services do not operate as a traditional telecommunication service. GSaaS enables private one-way transfer of data (space to ground or ground to space), does not have a hub station, and does not enable ground to space to ground communication. Hence, GSaaS is not similar to a satellite communication service like a VSAT or GMPCS service, wherein the equipment used (for example, a hub station) and the purpose for which it is typically used are entirely different

from the GSaaS service offering as well as the use cases for which it is intended. In contrast, GSaaS supports services that require one-way transfer of data for non-telecom purposes such as:

a. Earth observation – weather (analysing downlinked weather data to predict patterns) or natural disaster (analysing downlinked data during natural disasters to identify survivors and assess structural damage) prediction;
b. Telemetry tracking and control (TT&C) data, encompassing data related to the health and status of the satellite, and the determination of the exact location of the satellite;
c. Command function (up linking commands for control of satellite), etc.

Ground stations for the above purposes require authorisation from IN-SPACe. We believe that introducing a separate and additional authorisation framework for GSaaS earth stations, over and above that of IN-SPACe, will hinder the broader aim of enabling a vibrant space and satellite communications industry, with the objective of increasing private participation in the sector. We respectfully suggest that any GSaaS regulatory framework by Department of Telecom be reconsidered.

GSaaS uniquely enables faster scaling of satellite-based services, as it leads to the proliferation of satellite-based services without the costs involved to set up infrastructure. GSaaS also enables the provision of cost-effective resilient, ubiquitous, and seamless connectivity for IoT devices to run efficiently. IoT operators can harness the benefits from satellite communications, such as the ability to operate across a vast geography, connect remote assets, and downlink their data onto cloud storages. For satellite operators, engaging GSaaS is much cheaper than setting up their own earth stations. This demonstrates the need for a regulatory framework for GSaaS operators that allows satellite operators to harness the value of space-led innovation, where GSaaS is seen as a unique model that brings value to satellite-led research, separate from the traditional telecom-related use cases of satellites.

IAMAI Recommendation

Introduction of a separate and additional authorisation for GSaaS earth stations should be avoided. The Department of Space (DoS) and IN-SPACe should be the enabling and regulating agency for GSaaS earth stations. The DoT should not create onerous compliance obligations on GSaaS operators, including setting specific contractual terms for GSaaS operators and their customers (i.e., satellite operators) and any other third parties, or placing restrictive conditions pertaining to the relationship between the GSaaS operator and the satellite operator, as they will impact accessibility of satellite services.

Q10. Whether there is a need to introduce an authorisation under Section 3(1)(b) of the Telecommunications Act, 2023 for establishing, operating, maintaining or expanding cloud-hosted telecommunication networks, which may be used to provide telecommunication network as a service to the authorised entities under Section 3(1)(a) of the Telecommunications Act, 2023? If yes, what should be the eligibility conditions, area of operation, validity period of authorisation, scope, and terms & conditions (general, technical, operational, security etc.) of such an authorisation? Kindly provide a detailed response with justifications.

The Ministry of Electronics and Information Technology is tasked with developing policies for information technology and the internet under the Allocation of Business Rules8[6]. Cloud computing is an IT related service, and consequently, the governance of Cloud Service Providers (CSPs) in any form falls squarely within the jurisdiction of MeitY. Further, we do not believe an additional authorisation is needed for CSPs due to the following reasons:

1. **CSPs are sufficiently regulated under existing laws:** CSPs are already subject to comprehensive regulation under both existing general and sector-specific laws and regulation, including in the areas of security (Information Technology Act, 2000), consumer protection (Indian Contract Act, 1872; Consumer Protection Act, 2019) and privacy legislation (Digital Personal Data Protection Act) and proposed Digital India and Digital Competition legislations by MeitY and Ministry of Corporate Affairs respectively. MeitY also provides guidelines and requirements for cloud services for empanelment under its GI Cloud (MeghRaj) cloud computing initiative[7]. CSPs are required to demonstrate compliance with prescribed standards on security, interoperability, data portability and other conditions for empanelment[8], and such compliance is verified through audits conducted by the Standardised Testing and Quality Certification Directorate under MeitY. Regulators like the Reserve Bank of India and the Insurance and Regulatory Development Authority of India, also issue IT outsourcing guidelines to ensure that sector specific requirements and expectations continue to be met by regulated entities when they outsource IT, including when they adopt cloud. MeitY's Computer Emergency Response Team (CERT-In) has also introduced guidelines for CSPs including maintenance of ICT logs, customer records. Existing regulations allow access by law enforcement agencies in a streamlined manner, that may arise from a national security perspective. Further, the network infrastructure through which cloud services are accessed by customers is already regulated by Department of Telecom (DoT) for the Telecom Service Providers (TSPs).

2. **Cloud services form a part of a growing market segment and must not be subjected to extensive regulation that could hamper availability of cost-effective cloud services to Indian customers.** As iterated above, CSPs are already subject to and required to comply with a number of laws in India. There is no clear reason why CSPs and the cloud industry in general must be subject to specialised regulations when they are already compliant with applicable laws, such as data privacy and information security, which apply to all other computer systems functioning in India. Such regulation would raise costs for Indian customers and impede India's goal of becoming a global hub for cloud computing, content hosting and delivery[9].

3. **There are fundamental differences between TSPs and CSPs.** TSPs provide the infrastructure for connectivity and the connectivity itself. On the other hand, cloud services rely on the networks of TSPs to provide services to its users and therefore, do not control access to the internet or the network layer. There are also inherent differences between cloud services and telecom services. Unlike a telecommunications service, cloud computing does not involve the

[6] Pg. 51, Government of India (Allocation of Business Rules) 1961 (as amended up to 04 April 2019), available at https://cabsec.gov.in/writereaddata/allocationbusinessrule/completeaobrules/english/1_Upload_1829.pdf
[7] https://www.meity.gov.in/content/gi-cloud-meghraj
[8] https://www.meity.gov.in/writereaddata/files/Empanelment-Cloud-Service-Offering-March%202024.pdf
[9] Para 2.2, pg. 12, National Digital Communications Policy, 2018, Department of Telecommunications, Government of India, http://dot.gov.in/sites/default/files/Final%20NDCP-2018_0.pdf

supply of connectivity to any person. The services offered by CSPs are not substitutable with telecommunication services offered by the licensed TSPs. Cloud services are not transformed into telecommunications services simply because they support certain telecom network functions. In fact, telecom network-related functions hosted on the cloud are fully managed and controlled by the licensed telecom service provider, ensuring that regulatory accountability remains with the telecom provider, not the CSP. CSPs merely offer the infrastructure and technical resources, while the telecom provider controls network operations, security protocols, and compliance with telecom-specific regulations. Thus, imposing licensing on cloud providers would not enhance regulatory oversight or security—it would only create unnecessary regulatory burdens without adding meaningful benefits.

4. **TSPs are regulated because there is 'bottleneck' infrastructure with 'natural monopoly' characteristics that cannot be easily replicated, creating an enormous barrier to competition.** As in the case of other industries with significant infrastructure costs and a physical distribution network such as energy, water, or railways, telecommunication involves access to special privileges (right of way) and scarce resources (spectrum and telephone numbers). Such issues do not exist for the cloud sector which has always been open, competitive and free from infrastructure bottlenecks and other structural features that necessitate regulatory intervention as in the telecom sector. Cloud computing in the telecom supply chain is part of a much larger IT industry which includes software and hardware providers and vendors. Extending the scope of the regulatory framework to capture private networks is not justified and would have significant negative effects on the sector. There is no actual evidence of market failure in the telecom industry that would justify regulatory intervention. In the absence of a genuine market failure, there is no justification for regulation. If a specific market failure is identified and it needs to be corrected, then it should be addressed through a targeted, proportionate and effective solution rather than applying blanket regulations from another sector.

IAMAI Recommendation

There is no requirement for a separate authorisation for operating cloud-hosted telecommunication networks. A DoT authorised entity such as a Telecom Service Provider (TSP) would be responsible for complying with the authorisation terms and conditions. They should be allowed to have the choice of using a cloud service provider as an alternative to on-premises infrastructure. This is in line with the Recommendations on the Framework for Service Authorisations to be Granted Under the Telecommunications Act, 2023[10], where TSPs are recommended to be allowed to have the choice of using a CSP empanelled by MeitY as an alternative to on-premises infrastructure, as mentioned above. Cloud providers are already regulated under existing laws and should not be treated at par with authorised entities providing telecommunication network services, in alignment with international practices.

[10] Page 206, TRAI Recommendations on the Framework for Service Authorisations to be Granted Under the Telecommunications Act, 2023, available at https://www.trai.gov.in/sites/default/files/Recommendation_18092024_0.pdf

Q17. Whether there is a need to introduce certain new authorisations (other than the authorisations discussed above) to establish, operate, maintain or expand telecommunication networks under Section 3(1)(b) of the Telecommunications Act, 2023? If yes,

(a) For which type of telecommunication networks, new authorisations should be introduced? (b) What should be the eligibility conditions, area of operation, validity period of authorisation, scope, and terms & conditions (general, technical, operational, security etc.) of such authorisations? Kindly provide a detailed response with justifications.

AND

Q20. What provisions should be included in the terms and conditions of various network authorisations under Section 3(1)(b) of the Telecommunications Act, 2023 to improve the ease of doing business? Kindly provide a detailed response with justifications.

AND

Q34. In case it is proposed for introducing certain new authorisations to establish, operate, maintain or expand telecommunication networks under Section 3(1)(b) of the Telecommunications Act, 2023, what should be the respective financial conditions for each of such authorisation(s)? Please provide a detailed response with justifications in respect of each network authorisation, separately.

Traditionally, licensed telecom service providers (TSPs) have been providing and managing networks for digital enterprises. However, rising consumer demands for 'feature enhancement' and 'real-time service delivery' have now necessitated leading-edge network architecture and quality, uninterrupted availability, control and scalability of networks of these digital enterprises for delivering uniform and world-class digital services to consumers worldwide.

As a result, digital enterprises (former customers) are now pursuing ownership, control, and management of these backend systems and private networks. Regulators in major economies such as Singapore, Japan, United States of America (USA) and the European Union (EU) have already recognised the immense potential for industry growth and investments and have accordingly provided a flexible regulatory approach allowing exemptions for digital enterprises to establish and manage their Private Enterprise Networks. This has in turn helped these major economies in competing in the global race of becoming digital hubs.

The flexible regulatory approach includes exemptions or relaxed regulations for global enterprises establishing and managing Private Enterprise Networks solely for internal use (not for public end users). Singapore, in particular, exemplifies a flexible regulatory environment that has attracted subsea cable investments. It offers a private use licensing exemption for entities not seeking to operate their infrastructure as TSPs but for their own exclusive use.

India's unified licensed framework (now being revamped by the Government of India in light of the 2023 Act) prevents non-licensed Digital Enterprises from owning or managing Private Enterprise Networks. This limitation hinders 'ease of doing business' (EODB) for Digital Enterprises in India, deters foreign direct investment (FDI) into India's digital sector and delays proactive adoption of state-of-the-art technology for consumer services and. There is clear evidence that this is holding India back with investment and innovation.

India's total data centre capacity in 2024 is estimated at only ~730 MWs. The standard benchmark for proportionate data centre capacity is population per MW. On this basis India has exponentially less data centre capacity than other destinations competing for data centre investment. India has less than one fifth of the proportionate data centre capacity available in competing destinations for data centre investment across the Asia Pacific, one sixth of the capacity available in rival destinations across EMEA, and only ~3% of the proportionate data centre capacity available in North America:

In addition, there is no separate set of 'eased-out' license conditions applicable for TSPs providing Private Enterprise Networks to Digital Enterprises. On the contrary, the current unified license requires such TSPs to comply with various technical and security conditions and limitations meant for public networks. This is generally argued to indicate that all license conditions apply to TSPs equally for public as well as private networks, even though several technical, security and other conditions in the license may not be commensurate with the 'captive, non-public' nature of Private Enterprise Networks. Moreover, such conditions applicable to 'public networks' are increasingly becoming incongruent with technological advancements and prevent India from benefiting from best-in-class technology, network architecture and business models in the digital sector. Additionally, the costs and operational limitations of such conditions ultimately impact services and end users, and investment, innovation and growth of the Indian digital ecosystem.

Given the challenges above, and in order to promote EODB, making India a digital hub, and promoting exponential infusion of FDI into the IT and telecom sector in India, TRAI may kindly consider recommending an exemption from 'authorization' under the Telecommunications Act 2023, allowing Digital Enterprises incorporated in India to own, establish and manage Private Enterprise Networks.

Importantly, the Telecom Act 2023 clearly anticipates that some services could and should be excluded from the telecom authorisation approach as follows as we therefore recommend that this approach be taken for such services:

> Section 3 (3) provides that "(3) The Central Government, if it determines that it is necessary in the public interest so to do, may provide exemption from the requirement of authorisation under sub-section (1), in such manner as may be prescribed."
>
> Section 56 2 (b) provides that "The Central Government may, by notification, and subject to the condition of previous publication, make rules not inconsistent with the provisions of this Act, to carry out the purposes of this Act... (2) In particular and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely... (b) the manner of exemption for providing authorisation under sub-section (3) of section 3."

Further we think it is pertinent to note that India currently stands at a critical juncture in the global AI revolution, facing an opportunity that transcends mere 'ease of doing business.' While India successfully leveraged the first Internet Revolution through strategic policy reforms, the emerging AI era demands

a new generation of progressive regulations. With global internet traffic surging 25% in 2023[11] due to AI training and inference requirements, the stakes are unprecedented.

Key success factors in this new landscape include ultra-low latency capabilities and frictionless global data flow. Countries that minimise regulatory barriers and eliminate unnecessary intermediaries will attract major data centre investments. To this end, we propose establishing 'Special Cloud Transit Zones,' modelled after Special Economic Zones, where Transit Cloud Service Providers can operate with minimal regulatory burden. These zones would enable direct submarine cable landings, data centre establishments, and seamless connectivity - positioning India as a major global transit hub.

This strategic approach aligns with the National Digital Communications Policy 2018's vision of making India a global hub for cloud computing and data communications. By implementing these targeted reforms now, India can capture the exponential economic and employment benefits of the AI hyperscale revolution, just as it did during the first Internet Revolution.

[11] Cloudflare 2023 Year in Review, see here: 12 December 2023, see here: https://blog.cloudflare.com/radar-2023-year-in-review/