Harish Krishnan
Managing Director and Chief Policy Officer
South and Southeast Asia

Cisco Systems (India) Pvt. Limited
First Floor, RMZ Infinity, Plot No 15
Phase IV, Udyog Vihar
Gurgaon, Haryana 122015
Email: harkris2@cisco.com

1 June 2026

Shri Atul Kumar Chaudhary,
Secretary, Telecom Regulatory Authority of India,
World Trade Centre, Nauroji Nagar,
New Delhi - 110029

Subject: Response to Telecom Regulatory Authority of India's Consultation Paper No. 07/2026 regarding the Proliferation of Public Wi-Fi networks in India ("Consultation Paper")

Dear Mr. Chaudhary,

Greetings from Cisco!

We would like to thank **Telecom Regulatory Authority of India** (TRAI/Authority) for initiating a consultation on the critical topic of public Wi-Fi networks in India. We appreciate the Authority's proactive approach to expanding digital connectivity and welcome the opportunity to share our insights and recommendations to support India's vision for a robust, secure, and future-ready wireless ecosystem. We would like to submit a formal response to TRAI's Consultation Paper.

For over 30 years, Cisco has been deeply committed to India's digital transformation. Our recent research, including the State of Wireless 2026 report, underscores the critical role of public Wi-Fi as a strategic growth engine for the nation. We believe that by treating public Wi-Fi as digital infrastructure, India can unlock significant economic value, foster innovation, and ensure seamless digital inclusion for all citizens.

Our submission outlines that a comprehensive framework is centered on seven key principles, including prioritizing security, quality, and user trust, while emphasizing the importance of modern standards like Wi-Fi 6E and Wi-Fi 7. We believe that a collaborative public-private partnership, tailored to specific geographic and use-case requirements, will be instrumental in achieving Bharat 6G Vision.

Cisco aims to productively collaborate with the Government of India in its mission to build a resilient and inclusive digital economy. We look forward to continued engagement with the Authority.

Warm Regards

Harish Krishnan

Submission to the Telecom Regulatory Authority of India (TRAI)

Consultation Paper No. 07/2026: Proliferation of Public Wi-Fi Networks in India (TRAI Draft)

PART I - EXECUTIVE SUMMARY AND RECOMMENDATIONS

India has been central to Cisco's story for 30 years. Cisco has worked alongside Government, academia, industry and civil society to support the country's digital transformation. Since 2015, Cisco has positively impacted more than 50 million lives in India through programmes spanning digital connectivity, digital skilling, cybersecurity, entrepreneurship and community resilience.

Through the Country Digital Acceleration programme, Networking Academy and the 40 Communities initiative, Cisco has been deepening this engagement. In Mumbai, Cisco launched a Centre of Excellence for AI, Networking and Entrepreneurship[1] with Confederation of Indian Industry (CII) to train 100,000 students over three years in AI and networking and is expanding a collaboration with NIIT Foundation to skill 2.7 million Indians in AI and cybersecurity by 2028. Cisco Networking Academy[2] has reached 3 million learners in India.

Cisco's inaugural State of Wireless 2026 report, based on interviews with 504 organisations in India, confirms that Wi-Fi has become a strategic growth engine. Over 85% of Indian organisations report improvements in operational efficiency from wireless investments, and 78% report positive revenue impact. Yet 98% also report rising complexity, security threats and talent gaps – underscoring the need for secure, well-designed public Wi-Fi infrastructure[3].

India's Connectivity Progress and the Public Wi-Fi Opportunity

India has achieved substantial scale in mobile broadband – crossing 1 billion broadband subscribers and among the world's highest per-capita data consumption[4]. Public Wi-Fi, however, remains a fraction of what comparable economies have deployed. There are approximately 4 lakh (400 thousand) PM-WANI hotspots in India. This is a significant increase from the 207,642 hotspots recorded as of July 2024[5], but remains well below the Bharat 6G Vision target of 50 million hotspots by 2030. The public Wi-Fi density is far below China, the United States, the United Kingdom. There is a strong case for an accelerated, quality-focused, security-first approach to public Wi-Fi proliferation[6].

Industry analysis indicates India has roughly 0.5 million public Wi-Fi hotspots in total, far below comparable countries on a per-million-population basis[7] (BIF submission to TRAI, February 2025)

The recent delicensing of the lower 6 GHz band (5925-6425 MHz) for low-power indoor use creates a strong foundation for high-performance next-generation Wi-Fi. A study by Telecom Advisory Services, commissioned by the Dynamic Spectrum Alliance (DSA), indicates that full allocation of the 6 GHz band

---

[1] Cisco Blogs, Ushering in a new era of social impact in India. https://blogs.cisco.com/our-corporate-purpose/ushering-in-a-new-era-of-social-impact-in-india-mumbai-joins-ciscos-40-communities-initiative

[2] Cisco Networking Academy. https://www.netacad.com

[3] Cisco, 'State of Wireless Report 2026: India country factsheet', https://www.cisco.com/c/dam/en/us/products/wireless/state-of-wireless-report/cisco-state-of-wireless-india-factsheet.pdf

[4] Telecoms Regulatory Authority of India, DoT 2025 Year End Review Press Release, https://trai.gov.in/notifications/press-release/trai-releases-broadband-subscriber-base-india-crossed-1-billion-100

[5] Telecoms Regulatory Authority of India, Draft "The Telecommunication Tariff (Seventy First Amendment) Order", 2025

[6] Telecom Talk, 'PM-WANI Crosses 4 Lakh Hotspots as Public Wi-Fi Use Surges Across India', https://telecomtalk.info/government-expands-public-wifi-network-pm-wani/1005923/

[7] Broadband India Forum, BIF's Comments on the Draft Telecommunication Tariff (Seventy-First Amendment) Order, 2025 dated 15th January 2025, https://www.trai.gov.in/sites/default/files/2025-02/BIF_03022025.pdf

(1200 MHz) for unlicensed Wi-Fi use could generate a cumulative economic value of approximately **USD 4.03 trillion** (roughly Rs 34.25 lakh crore) for India over the 2024-2034 period[8].

The practical benefits for India are significant and multi-dimensional. The 500 MHz of newly delicensed spectrum enables the deployment of next-generation Wi-Fi technologies such as Wi-Fi 6E, Wi-Fi 7 and beyond, delivering higher speeds, ultra-low latency, and expanded network capacity — capabilities that are foundational to data-intensive applications including 4K streaming, AR/VR, industrial automation, and smart infrastructure. By making this spectrum available without licence fees or auction costs, the policy also lowers the cost of deployment for ISPs and Wi-Fi providers, which can translate into more affordable internet services for end consumers. Further, the Wi-Fi Alliance's whitepaper on the "Global Economic Value of Wi-Fi" illustrates how this in turn drives economic growth for the country. [9]

The move aligns India with over 100 countries — including the United States, the United Kingdom, South Korea, and EU member states — that have already opened the lower 6 GHz band, removing a competitive disadvantage that had, among other consequences, prevented the launch of Wi-Fi 7-dependent consumer devices in the Indian market. Taken together, the delicensing of the lower 6 GHz band advances affordability, innovation, and digital inclusion simultaneously — and the case for extending this approach to additional portions of the 6 GHz band merits serious consideration as this consultation proceeds.

Therefore, Cisco would like to suggest the **following recommendations**:

1. **Treat public Wi-Fi as strategic digital infrastructure**
   Public Wi-Fi should be recognized as a critical complement to mobile broadband, enhancing indoor coverage, alleviating congestion, enabling affordable access, and promoting digital inclusion. Wi-Fi is foundational to future-ready networks supporting diverse use cases.

2. **Prioritize security, quality, and user trust**
   Mandate modern security baselines such as WPA3, strong encryption, session isolation, and network assurance, ensuring enhanced security and user confidence in public Wi-Fi environments.

3. **Adopt interoperable, low-friction authentication and seamless roaming**
   Move towards standards-based federated identity solutions and Passpoint/Hotspot 2.0 mechanisms to replace captive portals and OTP-based logins. For example, the Wireless Broadband Alliance (WBA) OpenRoaming initiative[10] supports seamless, secure onboarding, improving user experience and network trustworthiness.

4. **Strengthen backhaul first**
   Sustainable public Wi-Fi deployments require robust fiber and high capacity backhaul infrastructure. Leveraging BharatNet, municipal fiber, shared infrastructure, and streamlined

[8] Broadband India Forum, BIF's Comments on the Draft Telecommunication Tariff (Seventy-First Amendment) Order, 2025 dated 15th January 2025, https://www.trai.gov.in/sites/default/files/2025-02/BIF_03022025.pdf
[9] Wi-Fi Alliance, Global Economic Value of Wi-FI 2021-2025, https://6ghz.info/wp-content/uploads/2022/02/Global_Economic_Value_of_Wi-Fi_2021-2025_202109-1.pdf
[10] Wireless Broadband Alliance OpenRoaming, https://wballiance.com/openroaming

site access is essential to support the increased capacity demands of Wi-Fi 6E and Wi-Fi 7 networks.

5. **Differentiate deployment models by geography and use case**
   Tailor technical and commercial models to specific environments such as rural community access, dense urban areas, and large indoor venues. Cisco's portfolio, for example, includes diverse access points optimized for various densities and coverage needs, including directional antennas for large venues and high-density spaces.

6. **Promote public-private collaboration for scale**
   Governments should enable infrastructure and policy frameworks, while industry deploys, operates, and innovates. Standards provide the common foundation for interoperability and security. An ecosystem approach supports collaboration across stakeholders to build resilient public Wi-Fi networks.

7. **Build for the future**
   Embrace next-generation Wi-Fi technologies including Wi-Fi 6E and Wi-Fi 7, the delicensed 6 GHz band, AI-driven network management, and energy-efficient designs. We wish to highlight that Cisco's Wi-Fi 6E and Wi-Fi 7 access points deliver higher throughput, lower latency, enhanced security, and AI-powered automation to create a future-ready wireless ecosystem.

PART II -- RESPONSES TO CONSULTATION QUESTIONS

Q1. Supply-side barriers to Public Wi-Fi proliferation and needed policy or regulatory changes

Current key supply-side constraints include limited affordable backhaul, site access and right-of-way friction, uneven access to public infrastructure, fragmented deployment models, and inconsistent security and interoperability practices.

India's Optical Fiber Cable (OFC) network has grown to 42.36 lakh route km, and 2,14,843 Gram Panchayats now have broadband connectivity under BharatNet; yet fiber availability at the last mile remains a bottleneck for public Wi-Fi quality[11]. Fiber-ready building codes like the ones that exist in other countries can also be looked at for the speedy deployment of Wi-Fi.

Unified power billing for Wi-Fi infrastructure is also a major concern that needs to be addressed.
Policy should focus on enablers rather than new layers of complexity: simplified site approvals, easier access to public assets, harmonised state and local Right of Way (RoW) processes (single window), and standards-based technical guidance for secure, interoperable deployments (e.g., WBA OpenRoaming). Public Wi-Fi should be planned as part of India's broadband infrastructure, not as a stand-alone overlay.

[11] Telecoms Regulatory Authority of India, DoT 2025 Year End Review Press Release, https://trai.gov.in/notifications/press-release/trai-releases-broadband-subscriber-base-india-crossed-1-billion-100

Q2. Demand-side barriers to Public Wi-Fi uptake and needed policy responses

The primary demand-side barriers are user trust, convenience and quality perception. Many users associate public Wi-Fi with insecurity, poor speeds and fragmented login experiences. Cisco's State of Wireless 2026 India research found that 91% of Indian organisations experienced at least one wireless security incident in the past 12 months, and 56% report escalating wireless threats – Illustrating that security concerns are well-founded and must be proactively addressed[12].

Cisco recommends that demand-side policy emphasize user trust: secure onboarding, predictable performance, visible trust indicators, and simple, consistent access across trusted networks. The user experience should be as frictionless as possible, particularly for low-income users accessing digital public services.

Q3. Reasons for uneven deployment, including in remote areas, and solutions

Uneven PM-WANI deployment reflects differences in backhaul availability, site economics, institutional capacity and local anchor demand. Industry analysis notes that approximately 45% of PM-WANI hotspots are concentrated in Delhi, a region with already high broadband penetration[13].

Cisco recommends a segmented approach: **rural areas** should prioritise community access anchored to schools, health centers, community services centers (CSCs) and Gram Panchayats with reliable backhaul; **urban public spaces** should use municipal infrastructure and transit hubs with strong performance and security standards; **large indoor venues** (e.g., stadiums, auditoriums, concert halls, airports) should be served by enterprise-grade designs integrated with site operations.

Q4. PM-WANI changes to improve revenue certainty and sustainability for PDOs/PDOAs

From an ecosystem design perspective, sustainability improves when operating models are simple, technically robust and based on trusted user experience. The TRAI tariff order of June 2025 mandating ISPs to offer FTTH plans up to 200 Mbps to PDOs at no more than twice consumer retail rates is a welcome step. India should further promote shared authentication, management, security and roaming capabilities across small providers, reducing complexity and improving service consistency.

Q5. Other challenges faced by PDOs/PDOAs

Technical support burden, customer acquisition, security compliance and difficulty maintaining quality at scale are likely constraints. Shared platforms, professional system integration support and clear technical baselines can reduce operational fragmentation.

Q6. Need for improvements in authentication, authorization, roaming and payment under PM-WANI

This is a key area for improvement. India should evolve away from heavy reliance on fragmented captive-portal and repeated OTP logins, and encourage:

- Standards-based federated identity approaches (i.e. WBA OpenRoaming)
- Passpoint / Hotspot 2.0 mechanisms for automatic discovery and secure onboarding
- Trusted inter-network roaming

[12] Cisco, 'State of Wireless Report 2026: India country factsheet', https://www.cisco.com/c/dam/en/us/products/wireless/state-of-wireless-report/cisco-state-of-wireless-india-factsheet.pdf

[13] Broadband India Forum, BIF's Comments on the Draft Telecommunication Tariff (Seventy-First Amendment) Order, 2025 dated 15th January 2025, https://www.trai.gov.in/sites/default/files/2025-02/BIF_03022025.pdf

• Federated policy control for identity, authorisation and accounting
• Frictionless payment models for free or low-cost access

A modern framework based upon OpenRoaming as an Industry Standard, would preserve compliance and traceability while materially improving user experience.

Q7. Role of Government - direct hotspot funding vs. enabling backhaul and market-led rollout
Cisco supports a balanced model. Government's primary role should be to enable: expand backhaul readiness, simplify access to public assets, harmonise state and local processes, and support common trust and interoperability frameworks.

Direct public funding should be used selectively where market failure is clear, especially in underserved rural and remote areas or priority public-service locations.

International experience from South Korea, the EU (WiFi4EU) and the UK all demonstrate the value of targeted public-private partnership rather than uniform nationwide subsidy.

Q8. Differentiated rural vs. urban strategies
India should adopt distinct strategies for rural versus urban areas:

- **Rural:** focus on inclusion, public service access, low-cost shared usage, resilient backhaul and anchor institutions.
- **Urban:** focus on congestion relief, indoor coverage, commuter and visitor experience, smart city use cases and operational quality.
- **High-footfall venues:** enterprise-grade design with stronger assurance, security and analytics.

Q9. Measures to improve deployment and uptake in high-footfall outdoor and indoor areas
High-footfall areas demand quality, security and seamlessness enterprise-grade design for dense environments; robust fibre or high-capacity backhaul; modern Wi-Fi standards (Wi-Fi 6E/7) and quality-of-service mechanisms; better radio frequency planning and lifecycle management; simplified, secure onboarding and roaming; access to street furniture and venue infrastructure; and clear roles for venue owners, service providers and system integrators. Public Wi-Fi in transport hubs, campuses, hospitals and public venues should be planned as part of the site's digital infrastructure.

The current PM-WANI framework expects a fixed identifier (BSSID) to identify a hotspot, and any changes would require re-registration of the BSSID at the central registry. Modern Wi-Fi 6E and 7 standards utilize MBSSID to improve network discovery, but vendors will require flexible BSSID assignments to implement these specifications efficiently. Centralized BSSID registration required under PM-WANI's current framework creates rigid, fixed identifiers that hinder this flexibility. We recommend that instead, India should use dynamic mechanisms like hostnames to identify registered APs to better insulate the infrastructure from evolving standards. We further recommend that industry standards such as WBA OpenRoaming be leveraged to augment or replace the current PM-WANI BSSID-based framework, to rely on cryptographic certificates to identify the network. Taking this approach will remove the dependency on BSSID that has resulted in impediments from the rigidity of central registration.

Q10. Funding mechanisms if Government funds Public Wi-Fi

Funding should prioritise underserved areas, public-service points and common infrastructure that has shown to improve long-term viability – especially backhaul and site readiness.

Q11. Criteria for fund allocation and disbursement

Allocation should prioritise absence of existing viable service, public-service importance, sustainability of operations, quality and security readiness, and measurable outcomes including usage and reliability.

Q12. Whether backhaul/last-mile constraints are a major barrier and what governments should do

Public Wi-Fi performance depends on the quality of the underlying transport network. India's OFC network has more than doubled since 2019 to 42.36 lakh route km, and BharatNet has connected 2,14,843 Gram Panchayats[14]. However, last-mile fiber availability for public Wi-Fi hotspots remains insufficient in many locations.

Cisco recommends prioritising broader fiberisation and high-capacity backhaul; effective use of BharatNet and municipal fiber assets; easier and faster access to ducts, poles and public infrastructure; support for wireless backhaul alternatives where fiber is not immediately feasible; and better coordination across central, state and local authorities.

Q13. Government funding for last-mile connectivity in uncovered and underserved areas

There is a need for government to provide funding in underserved areas where market conditions do not support viable rollout. Support should focus on shared and reusable infrastructure enabling multiple services over time, rather than one-off hotspot deployment. Backhaul support, site preparation and access to common infrastructure create stronger long-term value.

Q14. Right of Way and public-place access challenges

The new Telecommunications (Right of Way) Rules, 2024 are a positive step, with RoW application disposal times falling from 448 days in 2019 to approximately 34 days in late 2025.

Cisco recommends continued simplification and harmonisation of state and local processes, time-bound approvals, transparent fees and standard access conditions for public assets including poles, transport infrastructure, municipal furniture and buildings.

Q15. Role of State Governments

States can play a major enabling role by aligning local permissions, facilitating use of public assets, integrating public Wi-Fi into state digital programmes, and identifying high-value public-service locations where connectivity has multiplier effects.

Q16. State role in last-mile connectivity and fibreisation

State governments should take initiative to improve the availability of last-mile connectivity as they can materially improve rollout conditions by encouraging city and town fiberisation, co-ordinating departments and making municipal and utility infrastructure easier to use for digital infrastructure.

Q17. Role of local bodies

[14] Telecoms Regulatory Authority of India, DoT 2025 Year End Review Press Release, https://trai.gov.in/notifications/press-release/trai-releases-broadband-subscriber-base-india-crossed-1-billion-100

Local bodies are critical because they control many of the sites and assets most relevant to public Wi-Fi: streamlined permissions, facilitation of public asset access, support for local anchor use cases, and coordination with service providers and system integrators.

Q18. Incentives for TSPs and ISPs to participate

TSPs and ISPs are more likely to participate when public Wi-Fi is seen as complementary to their networks. With average monthly wireless data consumption at 24.01 GB per subscriber and rising, public Wi-Fi can improve customer experience, offload traffic in dense areas and create enterprise and managed-service opportunities. Government Policy should support commercial flexibility, backhaul enablement and interoperable technical frameworks.

Q19. Incentives for bandwidth and backhaul provisioning

The most effective incentive for the provisioning of bandwidth and backhaul for public Wi-Fi is to lower the cost and complexity of infrastructure deployment: easier fiber rollout, access to public infrastructure, and targeted support in hard-to-serve areas. Shared infrastructure and neutral-host approaches also improves economics.

Q20. Incentivising private entities to deploy hotspots

Policy should focus on clarity: simple rules, predictable compliance, easy access to standards-based technology, and the ability to integrate public access with venue security and analytics.

Q21. Role of system integrators

System integrators can play a very valuable role. At scale, public Wi-Fi involves design, security, identity, policy management, analytics, interoperability, assurance, lifecycle support and integration with venue or public systems. Experienced system integrators help public bodies and private entities deploy more secure, scalable and interoperable networks, reduce operational burden and improve long-term sustainability.

Q22. User challenges in authentication and how to simplify while preserving security

Users are currently facing challenges. Authentication should be simplified but not weakened.

Cisco recommends trust-based, standards-based methods that reduce repeated manual steps while preserving security and compliance: secure identity federation, certificate-based onboarding where appropriate, encrypted connections and strong policy control. The goal should be a model in which secure choice is also the simplest choice for users. Mechanisms such as Passpoint should be used to minimize user friction while providing security and trust.

Q23. Need for a centralised authentication and payment platform

A common platform or federated framework can help if it improves interoperability, trust and scale without operational rigidity. Cisco would support a model that provides common trust, identity and policy functions while allowing multiple operators, venues and service providers to participate. The architecture should be open, standards-based, secure and future-ready.

Q24. Interoperability and seamless roaming; whether roaming should be mandatory and a super-aggregator is needed

Interoperability and seamless roaming are essential. The Government has already acknowledged the importance of enabling interoperability through roaming across different PDOA networks.

Users should not need to re-register repeatedly across trusted environments[15]. India should support a framework for interoperable roaming based on open standards and trusted identity exchange.

The principle should be roaming by design, not fragmentation by design. Whether this is delivered via a super-aggregator or another federated model is less important than the underlying principles: openness, security, scalability, interoperability and low user friction. Any model should avoid locking the ecosystem into proprietary silos.

The WBA OpenRoaming solution can enable a secure, seamless, and automated Wi-Fi onboarding service that enhances user mobility and connectivity, particularly in public and large venue environments. OpenRoaming eliminates the need for manual Wi-Fi selection and insecure captive portals by enabling users to connect automatically to trusted networks through a federation of access providers (such as airports, retailers, and public venues) and identity providers (including service providers and device manufacturers).

This federation uses industry-standard security protocols like WPA2 Enterprise and WPA3 Enterprise to ensure encrypted authentication and privacy. These are proven and peer-reviewed standards by the IEEE and Wi-Fi Alliance. This ensures that the solution provides broad compatibility for current and emerging wireless standards[16].

Q25. Monetisation models by geography

The most durable models combine connectivity with broader value: public service delivery, enterprise venue experience, managed services, analytics, digital inclusion and ecosystem partnerships.

Q26. Additional suggestions

India has a significant opportunity to make public Wi-Fi a trusted and future-ready layer of its digital infrastructure. Cisco respectfully recommends anchoring the next phase around seven principles:

1. Treat public Wi-Fi as strategic digital infrastructure
2. Prioritize security, quality and user trust
3. Adopt interoperable, low friction authentication and seamless roaming
4. Strengthen backhaul first
5. Differentiate deployment models by geography and use case
6. Promote public-private collaboration for scale
7. Build for the future

Cisco stands ready to support a collaborative approach to help India scale secure, interoperable, high-quality public Wi-Fi in line with the country's broader digital ambitions.

[15] Cisco, Open Roaming, https://www.cisco.com/site/us/en/solutions/networking/wi-fi-6-6e/openroaming/index.html
[16] Cisco Space, Open Roaming Configuration Guide, 2024, https://www.cisco.com/c/en/us/td/docs/wireless/spaces/openroaming/b-spaces-or-cg/m-overview.html

Cisco appreciates the opportunity to contribute to this important consultation and looks forward to continued collaboration with TRAI and the Government of India.

Our response is provided in good faith for general discussion and informational purposes only.

****