BIF's Response to Consultation Paper On the "Proliferation of Public Wi-Fi Networks in India" dated 27 April 2026 (CP)

Q1. What are the key supply-side constraints affecting Public Wi-Fi proliferation in India? What targeted policy or regulatory measures may be required to address these supply-side constraints? Please provide your response in detail with justification.

A. BACKGROUND TO RESPONSE TO Q1. THIS MAY KINDLY BE CONSIDERED AS BACKGROUND TO RESPONSES TO ALL OTHER QUESTIONS IN THE CP.

A1. Preliminary Observations

BIF submits that the Authority deserves all appreciation for initiating this timely and forward-looking consultation on the proliferation of Public Wi-Fi networks in India. The Consultation Paper (CP) reflects a comprehensive and balanced examination of the technological, economic, regulatory and socio-economic dimensions of Public Wi-Fi and correctly positions Wi-Fi not merely as a supplementary hotspot service, but as an increasingly important component of India's future broadband architecture. **The CP repeatedly positions Public Wi-Fi as a complementary access layer to mobile and fixed broadband networks.**

The CP demonstrates a deep understanding of emerging digital realities, including the rapid growth of data intensive applications, the increasing importance of AI enabled services, the need for affordable and inclusive broadband access and the growing global convergence between fixed broadband, Wi-Fi and mobile networks. Importantly, the CP also recognises that while India has achieved remarkable success in mobile broadband adoption, **the country's future digital ambitions will require a broader and more balanced broadband ecosystem capable of supporting high-capacity, low-cost and inclusive connectivity at scale.** By undertaking this consultation at a time when global broadband ecosystems are increasingly transitioning toward integrated fixed-mobile-Wi-Fi architectures, **TRAI has created an important opportunity to reassess India's Public Wi-Fi strategy** in light of evolving technologies, rising digital demand and long-term national digital competitiveness objectives.

A2. India at a Structural Inflection Point in Broadband Policy

The CP provides a compelling statistical and economic basis to argue that India is approaching a structural inflection point in broadband policy. The CP implicitly demonstrates that **while India has become one of the world's largest consumers of mobile broadband data, it continues to remain under-penetrated in fixed broadband and Public Wi-Fi infrastructure relative to the scale of its future digital ambitions.**

The CP repeatedly emphasises that broadband is no longer merely a telecom service but foundational national infrastructure supporting digital governance, AI, cloud computing, digital commerce, education, telemedicine, IoT systems and enterprise digitisation. The CP further recognises that India's digital economy growth now depends upon deeper broadband usage and not merely basic internet access.

A3. <u>The Structural Challenge of Over-Dependence on Mobile Broadband</u>

A particularly important structural issue emerging from the CP is the excessive dependence of India's broadband ecosystem on mobile broadband. TRAI explicitly notes that India is a "mobile-first country" with among the highest per-capita mobile data consumption globally. However, **the CP simultaneously acknowledges that mobile broadband inherently faces capacity constraints, congestion sensitivity, indoor coverage limitations, variable speeds, latency challenges and higher per-GB delivery costs compared with fixed broadband-supported Wi-Fi.**

Para 1.9 of the CP compares performance, scalability, and cost structures.of FTTH (as fixed broadband) and mobile broadband technologies. It states that *"Broadband services in India are delivered through multiple technologies, including Fibre to the Home (FTTH), DSL, cable broadband, 4G/5G mobile networks and satellite.* ***While each has distinct strengths, they differ in their performance, scalability, and cost structures. FTTH, as a fixed broadband technology, provides high reliability, assured bandwidth, and consistently superior speeds, along with very high network capacity and low latency, making it well-suited for data-intensive and real-time applications.*** *It also supports multiple devices simultaneously and offers virtually unlimited data, making it ideal for homes, enterprises, and high-demand environments.* ***In contrast, mobile broadband, while essential for wide-area mobility and personal connectivity, operates under capacity, speed and latency constraints, and typically exhibits high variability. It also faces challenges such as higher per-GB delivery costs, variable speeds, and congestion-sensitive performance, particularly in dense urban areas .****"*

This distinction becomes economically critical when one examines the underlying broadband consumption architecture globally. **Advanced broadband markets are predominantly fixed-broadband driven in terms of total traffic carriage. International broadband consumption patterns indicate that nearly 75–80% of total internet traffic worldwide is carried through fixed broadband and Wi-Fi networks and is consumed indoors (where higher frequency mobile signals of 4G/5G find it difficult to penetrate), while mobile broadband accounts for less than 20–25% of aggregate traffic.** This is because **high-volume applications,** such as video streaming, cloud computing, gaming, AI workloads, enterprise applications, AR/VR, IoT and large-file transfers, **are structurally more efficient on fixed and Wi-Fi-based networks than on mobile-only architectures.**

The CP strongly aligns with this global trend. TRAI repeatedly notes that Wi-Fi is designed to function as a high-capacity shared access layer anchored on fixed broadband infrastructure and operating on unlicensed spectrum. **The CP also recognises that Public**

Wi-Fi enables traffic offload from mobile networks, improved indoor connectivity, higher throughput, lower latency, better spectrum efficiency and support for dense multi-device environments.

A4. <u>The Per-User Traffic Consumption Differential</u>

This distinction becomes even more significant when analysed from a per-user traffic consumption perspective. The CP states that FTTH subscribers in India consume approximately 250–300 GB per month per subscriber. By contrast, typical mobile plans in India remain constrained by daily caps such as 1 GB/day or 1.5 GB/day, resulting in effective monthly consumption limits of roughly 28–42 GB under standard retail plans. **Thus, even based on conservative TRAI calculations, fixed broadband users in India consume roughly 6–10 times more data per subscriber than typical mobile users**, and globally, fixed broadband networks continue carrying the overwhelming majority of total internet traffic.

This is not accidental. It reflects a structural reality of broadband economics. High-capacity applications naturally migrate toward fixed and Wi-Fi ecosystems because cost per GB is dramatically lower, throughput is higher, latency is lower, capacity is scalable and spectrum constraints are minimal.

The CP itself quantifies the cost differential very clearly. According to the CP, the **average mobile broadband cost is approximately ₹8.18 per GB, whereas effective fixed broadband Wi-Fi cost may be as low as ₹0.27 per GB under high-usage conditions**. With Public Wi-Fi supported by fiber broadband backhaul, the cost to the average user will usually range between **₹1 to ₹2 per GB**. This is a very sizable benefit for the price sensitive Indian consumer and needs to be leveraged to the maximum. Additionally, there are "incremental social benefits" from Public Wi-Fi which cannot be negated. Any social benefit to the masses must be fully supported.

A5. <u>Long-Term Consequences of Inadequate Fixed Broadband and Public Wi-Fi Infrastructure</u>

This **economic asymmetry has major implications for India's future digital trajectory.** If India does not significantly expand fixed broadband and Public Wi-Fi infrastructure, several long-term adverse consequences may emerge.

First, **India risks developing a structurally shallow digital economy** where users remain connected but are unable to participate meaningfully in high-capacity bandwidth digital ecosystems. The CP itself notes that only around 20–25% of India's internet users presently engage in online commerce compared with over 85% in mature digital economies. This gap is not merely an e-commerce issue. It reflects limitations in sustainable broadband access, affordability, quality of experience and capacity-intensive usage.

Second, **a digital divide may intensify between users capable of accessing fixed broadband ecosystems and those dependent exclusively on mobile data.** The CP

directly recognises that rising digital needs, incomplete mobile coverage and mobile broadband costs continue making the internet inaccessible for many low-income households. TRAI specifically identifies Public Wi-Fi as an affordable shared-access mechanism capable of bridging this affordability gap. This is especially important because future digital services will increasingly become data-intensive. Without affordable high-capacity access layers such as Public Wi-Fi, large sections of India's population may remain excluded from meaningful participation in next-generation digital ecosystems.

Third, **over-dependence on mobile broadband alone may create long-term network-efficiency, spectrum efficiency and investment challenges.** The CP clearly states that Public Wi-Fi can offload traffic from licensed cellular networks, reduce congestion, improve latency, increase throughput, and avoid excessive capital expenditure on towers, small cells and spectrum augmentation. *From an economic standpoint, this means that Public Wi-Fi improves national spectrum efficiency while lowering the cost of broadband delivery.*

India is a technology neutral regime and a calibrated play is required to meet the diverse requirements in this vast subcontinent. It would be too simplistic to assume that a single communication technology, i.e.mobile broadband, can effectively meet the communication needs of this large digital economy, currently as well as in the future. Mobile-first does not mean mobile-only or predominantly-mobile ecosystem. A highly diverse and technology-neutral country like ours, must facilitate and support a calibrated deployment of various technologies including fixed WiFi, satcom etc in order to ensure that the digital divide is kept at the minimum.

Fourth, **India's competitiveness in AI, cloud services and digital exports may weaken if broadband depth remains inadequate.** The **CP notes that India's IT and IT enabled services sector contributes nearly 10% of GDP and increasingly depends upon reliable high-capacity broadband infrastructure.** A mobile-only broadband model may be insufficient to support the scale and intensity of future enterprise-grade digital workloads.

A6. <u>The Case for a Layered Broadband Architecture</u>

The CP, therefore, implicitly points toward a **layered broadband architecture** for India. Mobile broadband is indispensable for mobility and personal connectivity. However, mobile alone cannot economically sustain the long-term traffic intensity of a large AI-driven digital economy. While mobile is easy to rollout and very convenient while on the move, it is well established that in today's digital economy, 70–80% of data consumption happens in-building or from fixed locations, and this is steadily rising. It is also well known that the high frequencies that are essential for modern mobile technologies are challenged to penetrate into buildings. Moreover, many of the data-crunchy and bandwidth-intensive apps of today are consumed mostly indoors and not on the move. There is, therefore, **a compelling need for strong in-building WiFi /Public Wi-Fi capable of catering to the intensive data requirements of all customers.**

The **CP positions Public Wi-Fi as a "complementary connectivity layer" rather than merely an auxiliary hotspot service.**

The global experience discussed in the CP reinforces this conclusion. South Korea's broadband architecture integrates extensive fibre backhaul, municipal fibre systems, over 94,000 Public Wi-Fi locations, seamless roaming, AI-based security and continuous upgrades toward Wi-Fi 6 and Wi-Fi 7. A comparison between South Korea and India, will show that with 94,547 hotspot locations spread across just 1,00,000 sq km, South Korea achieves a deployment density of approximately 0.95 hotspots per sq km. India, by contrast, has approximately 4.65 lakhs hotspots across a vast geography of approximately 33 lakhs sq km, yielding a density of merely 0.14 hotspots per sq km. **This means that India's Wi-Fi density is less than one-seventh of South Korea's. Given that India's population is approximately 26 times that of South Korea, and its digital economy ambitions are correspondingly vast, this density gap is a structural deficit that directly constrains affordable broadband access, indoor connectivity and digital inclusion for hundreds of millions of Indians.**

Even on the yardstick/benchmark of population, we are grossly inadequate. On a scale of number of hotspots/per capita, while India has one sixth of global population, it has less than 0.001 % of the global Public WiFi hotspot population.

Similarly, the European Union's WiFi4EU initiative created more than 93,000 hotspots under a unified interoperable architecture with common SSIDs and roaming frameworks.

These countries are complementing mobile networks with dense fixed and Wi-Fi ecosystems.

A7. <u>Strategic Conclusion: Public Wi-Fi as Essential Digital Infrastructure</u>

TRAI explicitly states that India's current Public Wi-Fi footprint remains inadequate relative to its geography, population, youth demographic and digital demand potential. The CP therefore suggests that **India must now move beyond viewing Public Wi-Fi merely as isolated hotspot entrepreneurship and instead treat it as strategic digital infrastructure capable of deepening broadband usage, reducing affordability barriers, supporting AI-era applications, enabling inclusive digital participation, improving spectrum efficiency and strengthening India's long-term digital competitiveness.**

It is submitted that **Public Wi-Fi** should not be viewed merely as a hotspot deployment exercise or a limited entrepreneurial activity. It should instead be **recognised as an important distributed broadband access layer capable of complementing mobile broadband, improving affordability, enhancing indoor connectivity, enabling traffic offload, increasing digital inclusion and supporting India's broader digital economy objectives.**

The Authority deserves appreciation for correctly identifying that Public Wi-Fi proliferation in India is not merely a technology deployment issue, but a broader ecosystem and broadband architecture issue. The CP appropriately recognises that future digital growth, AI-enabled services, cloud applications, IoT ecosystems, AR/VR applications, digital commerce and

inclusive broadband access will require a deeper and more balanced broadband infrastructure framework. **In this context, Public Wi-Fi assumes importance not as a standalone hotspot activity, but as a complementary broadband access layer capable of supporting affordability, capacity enhancement, traffic offload and digital inclusion.**

B. KEY SUPPLY-SIDE CONSTRAINTS AFFECTING PUBLIC WI-FI PROLIFERATION IN INDIA

It is important to recognise that the **principal supply-side constraints affecting Public Wi-Fi proliferation in India are not limited only to operational issues such as hotspot availability, authentication mechanisms or device deployment. The more important constraints are structural in nature and relate to the absence of a converged and commercially aligned broadband ecosystem under which Public Wi-Fi is treated as a scalable and integrated component of India's overall broadband architecture.**

B1. Absence of ecosystem alignment on the role of Public Wi-Fi

As noted in the background submission above, the **CP repeatedly positions Public Wi-Fi as a complementary access layer to mobile and fixed broadband networks.**

However, one of the key supply-side constraints in India is the **absence of broad ecosystem alignment amongst stakeholders regarding the role of Public Wi-Fi in the future broadband architecture of the country.** At present, different stakeholders often view Public Wi-Fi through divergent lenses.

In particular, some stakeholders may perceive Public Wi-Fi as not required due to mobile broadband proliferation, or they may, for some reasons, downplay the role of Public Wi-Fi. They may not perceive Public Wi-Fi as complementing mobile networks through traffic offload, indoor capacity enhancement and affordable shared access. **This perception needs correction, else this itself becomes an important structural supply-side constraint because large-scale telecom participation and investment may remain limited unless there is an alignment of drivers.**

B2. Lack of Awareness Among Deployment Stakeholders as a Supply-Side Constraint

A significant but insufficiently recognised supply side constraint is the widespread lack of awareness among the very entities that the PM-WANI framework depends upon to deploy and scale Public Wi-Fi hotspots in India. Despite PM-WANI having been operationalised since 2021, awareness of the framework, its commercial structure and the role of its key enablers remains poor among the most important class of potential deployers, viz MSMEs and local businesses

Compounding this awareness deficit is the **near-absence of a visible, accessible and standardised PDOA discovery mechanism**. A prospective PDO who does become aware of PM-WANI faces immediate practical uncertainty, which PDOA should they approach, what services do PDOAs offer, what are the applicable tariffs, what device is required, what does it cost and who provides support if something goes wrong. The **absence of a national onboarding platform, a certified device registry and a standardised PDOA marketplace** means that even motivated potential PDOs frequently encounter friction severe enough to abandon the process entirely. **Device cost and availability present a further supply side dimension of this awareness constraint**. PM-WANI compliant devices remain insufficiently standardised, inconsistently available and in many cases commercially unattractive for small establishments operating on thin margins.

The **absence of a certified plug-and-play device ecosystem** with transparent pricing and reliable after-sales support directly suppresses deployment rates in precisely the establishment categories that the PM-WANI framework was designed to activate. **The Authority is accordingly urged to treat the awareness, discoverability and device ecosystem deficit as a substantive supply-side constraint requiring targeted regulatory recommendation, including the establishment of a national PM-WANI onboarding and discovery platform, a certified device and network registry with standardised pricing guidelines, and a structured PDOawareness programme coordinated with industry and local bodies.**

B3. **Need for standardised and recognisable Public Wi-Fi**

Linked to the lack of awareness at shop level, a major supply-side constraint is that **Public Wi-Fi in India has not yet evolved into a standardised and recognisable broadband service category**. As a result, hotspot deployment continues to remain fragmented and dependent largely upon isolated entrepreneurial initiative rather than evolving into a scalable retail broadband ecosystem.

If Public Wi-Fi is a complementary access layer, then the shops etc. must be able to get, through standard procedures, the Public Wi-Fi installation in their premises with the same ease as that of installing a home broadband connection.

B4. **Ecosystem fragmentation and interoperability gaps**

The existing ecosystem remains heavily fragmented between PDOs, PDOAs, App Providers and broadband providers without sufficient standardisation of interoperability, authentication, roaming, settlement and managed-service frameworks. Fragmented login experiences reduce usage levels and weaken commercial sustainability for hotspot operators. This increases operational complexity and reduces scalability.

B5. **Inadequate fiberisation and affordable backhaul availability for Public Wi-Fi**

Another important supply-side constraint is inadequate availability of fiber based broadband connection (FTTX) at the hotpsot location besides the lack of affordable backhaul. Public Wi-Fi can scale sustainably only where robust and affordable fixed broadband infrastructure exists. However, uneven fibre deployment, municipal permission delays, fragmented Right of Way (RoW) frameworks and limited shared infrastructure access (particularly in case of fiber) continue to constrain hotspot economics and expansion.

C. TARGETED POLICY AND REGULATORY MEASURES TO ADDRESS SUPPLY-SIDE CONSTRAINTS

The Authority may, therefore, consider a **broader and more converged regulatory approach under which Public Wi-Fi evolves from a fragmented hotspot activity toward a structured and scalable broadband access ecosystem.** The following measures are submitted for the Authority's consideration:

C1. **Regulatory anchoring of Public Wi-Fi as a complementary broadband infrastructure layer**

As noted in the background submission above, the **CP repeatedly positions Public Wi-Fi as a complementary access layer to mobile and fixed broadband networks.** While such recognition is a necessary first step, **recognition alone, without attendant regulatory consequence, may prove insufficient** to overcome the structural resistance that has historically constrained Public Wi-Fi proliferation in India.

The CP explicitly and repeatedly characterises Public Wi-Fi as a foundational component of India's future broadband architecture, as an affordable shared access layer for digital inclusion and as an essential enabler of AI era applications and high-density digital environments. If these analytical conclusions are accepted, then **Public Wi-Fi cannot be treated as a commercially discretionary activity by regulated entities**. BIF accordingly submits that the **Authority may consider recommending that Public Wi-Fi be formally designated as a Complementary Broadband Infrastructure Layer under India's National Broadband Policy framework, with the following regulatory consequences flowing from that designation**:

- **TSPs and ISPs be subject to a non-discrimination obligation in relation to the Public Wi-Fi ecosystem**, prohibiting practices that commercially or technically obstruct or suppress Public Wi-Fi as a complementary access layer. The TSPs and ISPs must treat Public Wi-Fi as a complementary layer to be enabled and not as a service to be suppressed.

- **TSPs and ISPs be required to facilitate traffic offload arrangements with Public Wi-Fi operators and PDOAs** through a structured facilitation framework, with terms to be

determined through a transparent regulatory process. **The CP's own acknowledgment that Public Wi-Fi improves spectrum efficiency and reduces congestion on cellular networks makes traffic offload not a commercial choice but a network architecture obligation consistent with the Authority's spectrum efficiency objectives**.

The national broadband planning frameworks, including coverage targets and reporting metrics, explicitly incorporate measurable Public Wi-Fi density indicators alongside mobile and fixed broadband metrics. Currently there is a huge gap in measurement, collection of data and reporting of data related to

1. Number of Public WiFi hotspots
2. Actual number of active users at each PDO/PDOA
3. Actual data consumed at each PDO/PDOA

This data must be made publicly available and reported. Without actual measurement of data and reporting of the same, the situation on ground can not be improved.

BIF requests that the Authority could maybe consider operationalising this , so that TRAI could report this in their Monthly /Quarterly Performance Indicator Reports.

The stark density gap between India and comparable economies such as South Korea provides a concrete evidential basis for setting such targets and for holding the ecosystem accountable. (based on Public WiFi hotspots target set by Bharat 6G Vision).

- The **public infrastructure, including government buildings, municipal assets, transportation hubs and utility infrastructure, be subject to facilitate access for Public Wi-Fi deployment.** This would directly address one of the most persistent supply side constraints identified in the CP, namely the difficulty that hotspot operators face in accessing physical infrastructure for deployment.

A well-structured complementary infrastructure framework can create aligned outcomes for TSPs, ISPs, venue operators, PDOAs and end users simultaneously, and regulatory facilitation may help align the outcomes. rather than leaving them to voluntary commercial negotiation.

C2. **Enable commercial establishments to have the right to procure managed Public Wi-Fi connectivity**

A key regulatory and structural intervention may involve enabling commercial establishments located in broadband-served areas to have the right to procure managed Public Wi-Fi connectivity from authorised entities (including TSP/ISP/PDOAs, etc) through transparent and standardised retail mechanisms.

In practical terms, TRAI may consider recommending that ISPs and Broadband Service Providers to **introduce standardised "Public Wi-Fi Enablement" plans.** Such plans may

include managed authentication, captive portal support, bandwidth partitioning, lawful traceability, roaming integration, security compliance and remote hotspot management.

This would allow commercial establishments such as shops, cafes, clinics, educational institutions and small enterprises to procure Public Wi-Fi connectivity through ordinary retail channels in the same manner as other broadband services. The establishment would therefore function more as a broadband customer rather than as an independent telecom operator, which **structure is now already allowed under the PM-WANI Public Wi-Fi framework.**

Such an approach can **materially alter the economics of hotspot proliferation by converting Public Wi-Fi from an isolated entrepreneurial activity into a scalable managed-service category. The framework may establish a facilitative right-to-procure architecture under which commercial establishments located in areas where fixed broadband infrastructure already exists can obtain managed Public Wi-Fi connectivity on transparent and non-discriminatory terms wherever technically feasible.** This approach may create a natural demand-pull mechanism for hotspot proliferation while preserving commercial flexibility and market-led deployment.

C3. **Certified plug-and-play PM-WANI compliant device ecosystems**

The Authority may further consider promoting **certified plug-and-play PM-WANI compliant device ecosystems**. Most small establishments are not technically equipped to independently configure authentication systems, roaming integration and security protocols. Accordingly, **interoperable hotspot devices, based on PMWANI Public WiFi based Roaming/Open Roaming, capable of remote provisioning and management by PDOAs or ISPs may substantially reduce deployment friction, including transparency and affordability in terms of cost.**

In this respect, TRAI may also consider encouraging **development of PM-WANI-ready broadband device ecosystems capable of supporting optional secondary SSID functionality wherever technically and commercially feasible. Such readiness may significantly reduce deployment friction and incremental infrastructure costs while enabling future scalability of managed Public Wi-Fi participation models.**

C4. **A "Public Wi-Fi Ready" framework for large public-facing premises**

The Authority may consider **recommending a "Public Wi-Fi Ready" framework for large public-facing premises, campuses and commercial establishments.** Such a framework need not mandate active hotspot deployment in every case. Instead, it may require that such premises remain technically capable of supporting interoperable Public Wi-Fi systems through broadband readiness, fibre access, power availability, mounting space and interoperability support.

It is reiterated that while mobile is easy to rollout and very convenient while on the move, it is well established that in today's digital economy, **70–80% of data consumption happens in-building or in fixed locations**, and this is **steadily rising**. It is also well known that the **high frequencies that are essential for modern mobile technologies are challenged to penetrate into buildings**. Moreover, many of the **data crunchy and bandwidth intensive applications** of today are **consumed mostly indoors** and not on the move. There is therefore **a compelling need for strong in-building Public Wi-Fi capable of catering to the intensive data requirements of all customers. We submit that TRAI could jointly, along with MoHUA & DoT perhaps, plan to facilitate implementation of NBC 2016-Amendment 3 and NBSC 2026 to allow upgradation of latest next gen Public WiFi (WiFi 6E & higher versions) inside buildings.**

C5. **Encourage interoperable managed-service architectures**

To improve scalability, TRAI may also consider encouraging interoperable managed service architectures. The present PM-WANI ecosystem remains highly fragmented. Accordingly, **standardised APIs, interoperable authentication systems, roaming frameworks and settlement architectures may be promoted**. There is a case for tokenization of hotspots using Distributed Ledger Technology to unlock the potential as well as to enable auto-roaming.

Gradual migration toward Passpoint/OpenRoaming type frameworks may also be considered so that users experience Public Wi-Fi as a seamless broadband layer rather than isolated hotspot islands requiring repeated authentication. **A national discovery platform/portal for PDOAs and hotspot service providers may also be considered so that prospective PDOs can identify providers, tariffs, onboarding processes and support systems.**

C6. **Stronger municipal and local body participation**

The Authority should encourage and recommend stronger municipal and local body participation. International experiences discussed in the consultation paper demonstrate that successful Public Wi-Fi ecosystems invariably rely upon active participation by municipalities and local authorities through access to street furniture, municipal fibre networks, smart-city integration, simplified permissions and public-space access. Accordingly, **municipalities and local bodies in India may be encouraged to function as enabling infrastructure facilitators with skin in the game rather than merely approval authorities.**

C7. Spectrum policy alignment and technology upgrade pathway as supply-side imperatives

An important supply-side dimension that merits specific regulatory attention is the need to align Public Wi-Fi deployment policy with India's evolving spectrum policy and the global

transition toward next-generation Wi-Fi technologies. The CP notes that the Government of India has issued a notification delicensing the lower 6 GHz band (5925–6425 MHz) for low-power indoor and very low-power outdoor use, and that TRAI has recommended delicensing of the V-Band (57–66 GHz) for low-power indoor and very low-power outdoor use. This spectrum development represents a significant structural opportunity for Public Wi-Fi proliferation in India, as the 6GHz as well as the 60 GHz (V band) band enables substantially wider channels, multi-gigabit speeds, reduced congestion and superior performance for data-intensive applications indoors compared with the already congested 2.4 GHz and 5 GHz bands.

However, spectrum availability alone is insufficient if the device ecosystem does not evolve in parallel. Wi-Fi 6E and Wi-Fi 7 capable devices i.e. access points, routers and client devices, remain relatively scarce and expensive in the Indian market, particularly at the price points accessible to small PDOs, local entrepreneurs and community-level hotspot operators. Accordingly, a key supply-side constraint going forward is not merely spectrum policy but device ecosystem readiness I.e. the availability, affordability and certification of 6 GHz capable Wi-Fi devices at scale in the Indian market. A suitable PLI scheme for Local Manufacturing of WiFi Devices at scale may be recommended.

BIF therefore submits that the Authority may consider recommending to the Government a coordinated approach to Public Wi-Fi technology upgrade that encompasses three elements.

First, facilitation of affordable access to Wi-Fi 6E and Wi-Fi 7 capable devices through measures such as import duty rationalisation, domestic manufacturing incentives under relevant production-linked incentive schemes and simplified type approval processes for certified devices.

Second, the gradual articulation of a technology upgrade pathway for Public Wi-Fi that encourages deployment of Wi-Fi 6E or higher generation systems in new high-footfall and public-service hotspot environments, so that the Public Wi-Fi ecosystem does not become locked into ageing technology at a time when global ecosystems are rapidly transitioning to higher capacity architectures.

Thirdly, **TRAI should jointly along with MoHUA & DoT plan to facilitate implementation of NBC 2016-Amendment 3 and NBSC 2026 to facilitate upgradation of latest next gen Public WiFi (WiFi 6E & higher versions) inside buildings**

(i) . Such a roadmap, even if initially expressed as a best-practice guideline rather than a binding obligation, would provide important directional clarity for ISPs, PDOAs, device manufacturers and infrastructure investors.

Q2. What are the major demand-side constraints limiting the uptake of Public Wi-Fi services in the country? What targeted policy or regulatory measures may be required to address these demand-side constraints? Please provide your response in detail with justification.

A. PRELIMINARY OBSERVATIONS

From the perspective of broadband adoption and usage, the principal demand side constraints limiting the uptake of Public Wi-Fi services in India relate primarily to end user behaviour, user experience, trust & safety , reliability and resilience of the connectivity and perceived utility of Public Wi-Fi services. It is important, however, to first recognise what are not demand side constraints There is no lack of demand for broadband itself. India already exhibits one of the world's highest levels of mobile broadband consumption and users increasingly depend upon digital services for commerce, entertainment, education, payments, communication and public services. **The more fundamental issue is that the majority of end users have not yet experienced a good quality Public Wi-Fi hotspot and hence do not perceive Public Wi-Fi as sufficiently seamless, reliable, trusted or differentiated when compared with mobile broadband. The demand-side challenge is, therefore, not one of insufficient digital appetite but of insufficient experience, awareness and confidence in Public Wi-Fi as a service category.**

It is also important to contextualise this challenge historically. **For over 25 years, Wi-Fi in India was not liberalised. The policy and regulatory environment did not permit the free and open development of a Public Wi-Fi ecosystem. PM-WANI, which opened this space, is a relatively recent framework. It is therefore neither surprising nor a reflection of structural weakness in the PM-WANI model that mass user awareness and adoption have not yet materialised. <u>What is needed is a combination of removal of regulatory challenges and entry barriers, ease of doing business, integrated awareness at national and state levels, simplified access, quality of service assurance for Public Wi-Fi and PM-WANI to establish themselves in the public consciousness.</u> The Authority's recommendations and the Government's acceptance of the same can play a decisive role in doing so.**

B. MAJOR DEMAND-SIDE CONSTRAINTS

B1. <u>Lack of end user awareness and discoverability</u>

A significant and insufficiently recognised demand-side constraint is the **widespread lack of awareness among end users**, the individuals who would benefit from and consume Public Wi-Fi services if they were aware of their existence, location and ease of use. Despite the rapid expansion of internet usage in India there are hardly any Public WiFi hotspots at all. Also, a large proportion of potential Public Wi-Fi users, particularly in semi-urban areas, among lower-income households and among first-generation internet users, remain

unaware that affordable Public Wi-Fi hotspots may be available in their vicinity,and that lawfully deployed PM-WANI hotspots operate within a regulated framework that includes security and traceability standards.

Limited uptake of Public Wi-Fi hotspots that exist today, is largely due to very poor awareness of the many superior economic and quality benefits available to the customer through the use of Public Wi-Fi backed by a fixed fibre-based broadband connection. It can easily be demonstrated that such a fixed broadband connection with modern Public Wi-Fi would benefit the end user significantly on both the quality and economic fronts. Many users remain **unaware of nearby hotspots**, **of the availability of PM-WANI services, or of the potential advantages of Wi-Fi-based broadband access in terms of speed, affordability and data-intensive usage**. The Central and State Government are required to launch a mass awareness campaign on the scale of say " A Swachh Bharat Mission" and the Regulator is kindly requested to use his good offices to initiate awareness through its nationwide consumer awareness campaigns to create the informed user base that the PM-WANI ecosystem requires to achieve scale.

B2. **Fragmented and friction-heavy user experience**

India's mobile broadband ecosystem has evolved into an always on, highly integrated and frictionless consumer experience. Users are accustomed to automatic connectivity, unified billing, persistent authentication and seamless mobility. Public Wi-Fi networks, by contrast, are often perceived as fragmented and inconvenient because users may be required to search for hotspots, repeatedly authenticate through OTPs, download applications, purchase vouchers, re-login at multiple locations or navigate inconsistent captive portal experiences. As a result, even where hotspots exist, actual usage levels may remain significantly below potential. Public Wi-Fi presently lacks sufficiently differentiated consumer positioning, and users who perceive mobile broadband as good enough for ordinary usage may naturally continue defaulting to mobile networks. This **perception is, however, a consequence of fragmented and low-scale deployments and does not reflect the true capability of a well-deployed Public Wi-Fi system, as the global examples cited in the CP demonstrate.**

B3. **Inconsistent quality of service**

A major demand-side constraint is inconsistent quality of service. In many cases, users encounter variable speeds, unstable connectivity or overloaded hotspots. This reduces confidence in Public Wi-Fi as a reliable broadband alternative for high-bandwidth applications. International experiences discussed in the CP demonstrate that sustained Public Wi-Fi adoption depends significantly upon quality consistency and user confidence in service performance. Successful Public Wi-Fi ecosystems such as those in South Korea, UK and the European Union have generally evolved around high-capacity fibre supported architectures combined with predictable user experience standards. The WiFi4EU programme in the European Union established minimum speed expectations of 30 Mbps for

supported hotspots, while South Korea progressively upgraded Public Wi-Fi systems through dense fibre backhaul and Wi-Fi 6/Wi-Fi 7 infrastructure. These examples suggest that **users become habitual and regular consumers of Public Wi-Fi services only when the connectivity experience is perceived as reliable, high-quality and materially useful for data-intensive applications.**

B4. **Lack of service continuity and interoperability**

Another demand-side constraint relates to lack of service continuity and interoperability. Users moving across locations frequently experience disconnected hotspot environments requiring repeated authentication and onboarding. This reduces the perception of Public Wi-Fi as a dependable broadband layer and reinforces user preference toward mobile networks. A national broadband access layer that requires the user to re-authenticate at every location cannot compete in user experience with a mobile network that follows the user seamlessly. Until Public Wi-Fi begins to function as a connected and interoperable ecosystem rather than a collection of isolated hotspot islands, demand will remain constrained by this structural experience deficit.

B5. **Trust and security perceptions**

Trust and security perceptions are huge challenges in adoption of Public WiFi. There are several recent advisories from various Government departments asking the citizens not to use Public WiFi as it is a security risk.

[BIF has analysed the issue in its Cyber Security Committee and has attached a detailed note which is enclosed in Annexure I .]

Such advisoriesmaterially affect willingness to connect, particularly for digital payments, enterprise usage and sensitive transactions. It is important to address this perception with factual clarity.

Modern Wi-Fi ecosystems, including those employing OpenRoaming or PM-WANI compliant architectures, provide a high degree of trust and security. Most cyber frauds in India today are perpetrated over conventional mobile and broadband internet connections, including private mobile networks and home or enterprise Wi-Fi systems, rather than through public Wi-Fi hotspots. Available evidence does not indicate that public Wi-Fi systems are a disproportionately significant source of cyber fraud. Secure financial transactions are possible in a reliable manner through modern PM-WANI based Wi-Fi hotspots, and most websites accessed today are of the https category and are therefore secure. [Please refer to detailed Note on WiFi Security in Annexure I] Today's technologies are continually advancing and security concerns should be treated as reasons to improve the architecture, not as grounds for condemning or dismissing Public Wi-Fi.

C. TARGETED POLICY AND REGULATORY MEASURES TO ADDRESS DEMAND-SIDE CONSTRAINTS

C1. Coordinated public awareness programme

Given that over 25 years of regulatory restriction prevented the development of a Public Wi-Fi culture in India, the most urgent demand side intervention is a coordinated and sustained public awareness programme. The Authority and the Government may jointly develop and disseminate communications that clearly articulate the availability, affordability, ease of use, quality advantages and regulatory safety standards of PM-WANI compliant Public Wi-Fi. Such communications should specifically address the economic and quality benefits of Public Wi-Fi backed by fixed fibre broadband, counter misconceptions regarding security and compare the cost-per-GB advantage of Public Wi-Fi over mobile broadband in terms that are immediately meaningful to price-sensitive users. The Authority's role, along with that of the Government's, in this regard carries particular weight in the context of any contrary commercial narrative that may seek to discourage Public Wi-Fi adoption.

C2. Frictionless authentication and unified discovery

Demand-side interventions should focus primarily upon improving user experience, trust, service continuity and perceived utility. One important approach is gradual migration toward frictionless authentication architectures such as Passpoint/OpenRoaming and persistent device-based authentication systems. Under such frameworks, users may authenticate once and thereafter connect automatically to participating hotspots without repeated OTP or login procedures. This may be operationalised through interoperable authentication frameworks managed through PDOAs, federated platforms or neutral clearing-house systems. The objective should be to ensure that Public Wi-Fi begins functioning as a seamless connectivity layer rather than as isolated hotspot islands.

Here it may be prudent to mention that recently DoT has released a series of measures to improve the demand side challenges. One of the major ones is wherin it has mandated all PDO/PDOAs to have a standardized hotspot branding, unified discovery systems and interoperable hotspot maps. A visible and trusted national Public Wi-Fi identity may improve user confidence and awareness. UPI-integrated one-click micro-payment systems may additionally improve onboarding convenience. Instead of complex voucher purchase systems, users may authenticate and make payments through simplified UPI-based flows embedded directly within hotspot onboarding systems.

C3. Quality - best practice standards

TRAI may consider encouraging gradual development of best-practice and uniform equipment specifications for Public Wi-Fi deployments, particularly in high-footfall locations, public institutions, transport hubs, educational campuses and dense urban environments.

Such an approach may help **improve user confidence, increase repeat usage and strengthen perception of Public Wi-Fi as a dependable broadband access layer rather than merely a fallback connectivity option.** At the same time, any such framework should remain proportionate and flexible so that compliance burdens do not discourage participation by smaller PDOs or local hotspot operators.

C4. **Security and trust enhancement**

Security and trust enhancement will be critical to sustained demand-side growth. Accordingly, **interoperable security certification frameworks, use of techniques such as client isolation, stronger adoption of WPA3 standards, secure authentication protocols and visible trust markings may be encouraged**. **Public awareness campaigns regarding safe usage of duly certified Public Wi-Fi networks by a competent Authority to be nominated by the Government and the Regulator, may also improve consumer confidence.**

A recognisable national trust mark for PM-WANI compliant hotspots, analogous to a quality certification, may significantly reduce user hesitation, particularly for digital payments and sensitive transactions. A nationally recognised trust mark, analogous in concept to the BIS certification mark for physical products or the Jago Grahak Jago programme for consumer awareness, applied to certified PM-WANI compliant hotspots that meet minimum standards of authentication, security, traceability, uptime and service quality would give users an immediately recognisable visual signal that a hotspot is safe, regulated and trustworthy. The international precedent is well established. The EU WiFi4EU programme required participating hotspots to carry common branding and meet minimum performance standards, which materially improved user confidence and adoption. South Korea similarly uses standardised hotspot identification across its national public Wi-Fi ecosystem. I**n the Indian context, a trust mark framework could initially be voluntary, applicable to PDOAs and hotspot operators who demonstrate compliance with a defined set of minimum standards, and could progressively become the recognised quality signal for the PM-WANI ecosystem. The Authority may therefore consider recommending to the Government the development of a national Public Wi-Fi quality certification framework administered through an appropriate body, with a visible and standardised trust mark that certified hotspots may display both physically and digitally within their onboarding interfaces.**

C5. **Use-case differentiation and commercial bundling**

An important demand-side intervention involves creation of stronger use-case differentiation. Public Wi-Fi may achieve greater adoption **where users experience meaningful advantages over mobile broadband, particularly in high-footfall locations, transport hubs, educational campuses, hospitals, public institutions, tourism zones, dense indoor environments and high-capacity usage scenarios such as streaming**

and large downloads. Commercial bundling models may also help improve user adoption. Cafes, restaurants, retail establishments, transport operators and commercial venues may **bundle Wi-Fi access with purchases or customer engagement programmes, thereby improving both hotspot utilisation and retail value creation.**

C6. **Seamless roaming and interoperability**

The Authority may additionally consider encouraging interoperable roaming frameworks so that users experience continuity across hotspot networks. A **national roaming platform interconnecting PDOAs could significantly improve seamless usage and continuity of PM-WANI services**. Seamless roaming may significantly improve user perception of Public Wi-Fi as a dependable national broadband layer. PM-WANI can also play a vital role in crowded locations such as Kumbh Melas, stadiums, Rath Yatras and transport hubs where mobile networks experience congestion, and may additionally be encouraged in ASI heritage sites, tunnels, underground parking areas, trains and aircraft using satellite or Air-to-Ground connectivity. Bundled monument tickets with one hour of PM-WANI based Public WiFi access service can also be sold. This will help in larger adoption of Public WiFi hotspots.

C7. **Support for foreign tourists and visitors**

PM-WANI presently does not adequately support foreign tourists using foreign SIM cards because OTP based authentication is dependent on Indian SIMs. This is a significant gap that reduces the utility and visibility of PM-WANI in precisely the high-footfall, high-visibility environments I.e. airports, tourist centres, metro stations and heritage sites, where it could create the strongest positive impression. A **suitable onboarding mechanism for foreign visitors** at such locations may be considered, which would both expand the user base and **improve India's digital hospitality credentials.**

D. **A Phased Strategic Roadmap for Public Wi-Fi Mainstreaming**

Given the structural and behavioural nature of Public Wi-Fi adoption challenges in India, the Authority may also consider whether a **phased strategic roadmap for Public Wi-Fi mainstreaming** would be useful in addition to isolated policy interventions. Such a roadmap need not focus primarily upon numerical hotspot targets alone. International experiences discussed in the CP suggest that **sustainable Public Wi-Fi ecosystems evolve through gradual behavioural adoption, ecosystem integration, interoperability, quality consistency and institutional participation rather than merely through hotspot proliferation.**

In the **initial phase**, emphasis may be placed upon **hotspot discoverability, common branding, simplified onboarding and a trusted usage experience in high-visibility public environments such as transport hubs, educational campuses, markets and public institutions.** Subsequent phases may **progressively focus upon interoperable**

roaming, seamless authentication, managed-service architectures, municipal integration, and enterprise participation

Over time, such an approach may enable Public Wi-Fi to evolve from fragmented hotspot availability toward a mainstream and habitually used broadband access ecosystem integrated with India's broader digital connectivity architecture.

Given that Public Wi-Fi was restricted in India for over 25 years, the ecosystem deserves a sustained, well-supported and fair opportunity to demonstrate its full potential to the Indian user.

Q3. Despite the PM WANI initiative, scaling the number of public hotspots across diverse geographies, especially in remote and underserved regions, remains uneven. What are the key challenges in expanding both the density and geographic spread of hotspots, and what strategies could help accelerate more balanced, nationwide coverage? Please provide your response in detail with justification.

A. FRAMING THE ISSUE: DENSITY, GEOGRAPHIC SPREAD AND SPATIAL PLANNING

This question being different from the broader supply-side and demand-side issues addressed in Questions 1 and 2, we understand that this question is concerned specifically with the physical and geographic proliferation of Public Wi-Fi hotspots across India. It requires examination of why hotspots are not emerging with adequate density in high-demand areas and why their geographic spread remains uneven across rural, semi-urban, remote and underserved regions.

Accordingly, the issue is not merely one of increasing the total number of hotspots. The **more important policy issue is how India can transition from scattered and fragmented hotspot deployment to a planned, spatially distributed and commercially sustainable Public Wi-Fi access layer.** In this sense, **hotspot proliferation must be viewed as a spatial infrastructure planning issue, similar to planning of fibre routes, mobile towers, transport nodes, street lighting, public utilities and digital public infrastructure.**

The challenges relating to hotspot density and geographic spread are different in nature. Density is primarily an urban, semi-urban and high-footfall issue. It requires creation of clusters of hotspots in locations where users move, work, transact, study, travel or gather. Geographic spread, on the other hand, is an inclusion issue. It requires extending Public Wi-Fi to remote, rural and underserved areas where commercial viability may be weak but social and economic value may be high.

B. KEY CHALLENGES IN EXPANDING DENSITY AND GEOGRAPHIC SPREAD

B1. Fragmented and location-specific deployment

The first major challenge is that Public Wi-Fi deployment in India has remained largely fragmented and location specific. Hotspots tend to emerge where an individual entrepreneur, institution or service provider sees a limited business case, rather than as part of a planned broadband access network. This leads to scattered availability, weak continuity and low user habit formation. Isolated hotspots do not create the same user value as dense hotspot zones or Wi-Fi corridors.

B2. Absence of spatial planning

The second major challenge is lack of spatial planning. At present, there is no sufficiently institutionalised mechanism under which hotspot locations are planned based on footfall, public service importance, fibre availability, commercial activity, tourism potential, educational need, transport usage and underserved status. In the absence of such planning, hotspot deployment may not align with actual public need or usage potential.

B3. Weak integration with local infrastructure

The third challenge is weak integration with local infrastructure. Public Wi-Fi requires access to poles, street furniture, public buildings, bus shelters, railway stations, markets, campuses, municipal fibre, electricity supply and safe mounting locations. These assets are largely controlled or influenced by local bodies, transport authorities, public institutions and other public agencies. Unless these entities are actively integrated into the deployment framework, hotspot expansion will remain slow and uneven.

B4. Inadequacy of last-mile backhaul in rural and underserved areas

The fourth challenge is the inadequacy of last-mile backhaul in many rural and underserved areas. Public Wi-Fi hotspots require reliable backhaul, and without fibre or other adequate backhaul, hotspot deployment becomes either technically weak or commercially unviable. The CP itself recognises that Public Wi-Fi is supported by robust backhaul infrastructure and that India's current footprint remains inadequate in relation to its geography, population and digital demand.

B5. Absence of a differentiated strategy for different geographies

The fifth challenge is the absence of a differentiated strategy for different geographies. A single model cannot work equally for metropolitan markets, rural villages, tourist locations, transport hubs, educational campuses and remote areas. Urban density may be market-led, rural spread may require anchor institutions and public support, and high-footfall locations may be best suited for public-private partnership or venue-led models.

C. LESSONS FROM INTERNATIONAL EXPERIENCE

The international examples discussed in the CP support this view. South Korea's success was built not merely on hotspot numbers but on integration of Public Wi-Fi with municipal fibre, public facilities, transport systems, smart-city infrastructure, seamless access and continuous technology upgrades. Seoul's municipal fibre networks and approximately 34,000 Public Wi-Fi hotspots demonstrate the importance of city-level planning and local government execution. The EU's WiFi4EU programme similarly used municipalities as the deployment anchor, funded hotspot installation through vouchers and required common branding and minimum performance standards. These examples show that balanced Public Wi-Fi proliferation requires institutional execution models, not merely policy permission.

D. STRATEGIC FRAMEWORK: A PUBLIC WI-FI SPATIAL PLANNING APPROACH

India may therefore consider a **Public Wi-Fi Spatial Planning Framework**. Under such a framework, **hotspot planning may be undertaken at district, municipal, town and Gram Panchayat levels based on objective parameters such as population density, footfall, public service delivery points, educational institutions, health facilities, markets, transport nodes, tourism locations, fibre availability and digital inclusion gaps.**

D1. From isolated hotspots to hotspot clusters

The first strategic step should be to move from isolated hotspots to hotspot clusters. Public Wi-Fi is more useful when users experience predictable availability across a zone rather than a single point of access. **Deployment may therefore be prioritised in identified Wi-Fi zones such as markets, bus terminals, railway station areas, university areas, hospital districts, tourism zones, commercial streets, public parks and government service centres.** Such clustering will improve user familiarity, increase usage, create better commercial economics and support seamless roaming over time.

D2. Creation of Public Wi-Fi corridors

The second strategic step should be creation of Public Wi-Fi corridors. These may include **tourism circuits, religious circuits, public transport routes, educational corridors, industrial clusters, commercial markets and rural service corridors.** Such corridors can be planned around movement patterns rather than administrative boundaries. This is particularly relevant for India because many users require connectivity not only at one location but across movement paths.

D3. Anchor institution model for rural and underserved areas

The third strategic step should be the anchor institution model, especially for rural and underserved areas. Instead of expecting immediate commercial deployment everywhere, **Public Wi-Fi may first be deployed at institutions that already function as community**

access points. These may include Gram Panchayat offices, schools, colleges, primary health centres, Common Service Centres, post offices, railway stations, bus stands and local government offices. Once these anchors are connected, nearby commercial establishments may be encouraged to extend the Public Wi-Fi layer.

D4. Integration with BharatNet, state fibre networks and Smart City infrastructure

The fourth strategic step should be integration with BharatNet, state fibre networks and Smart City infrastructure. BharatNet-connected Gram Panchayats and state fibre grids can provide the backbone for rural and semi-urban Wi-Fi expansion. Similarly, Smart City infrastructure already includes fibre, command centres, CCTV networks, power availability and street assets. Public Wi-Fi can often be added to such infrastructure at marginal incremental cost if coordination is institutionalised.

The long-term success of rural Public Wi-Fi proliferation may depend significantly upon **deeper operational integration between BharatNet and PM-WANI ecosystems.** BharatNet may progressively evolve not merely as a fibre deployment initiative, but as an active and open-access rural broadband distribution backbone capable of supporting scalable last-mile Public Wi-Fi ecosystems. In this regard, transparent wholesale access frameworks, defined service-level standards, uptime accountability and simplified access arrangements for licensed ISPs may materially improve utilisation of BharatNet infrastructure.

Simultaneously, India may benefit from **gradual extension of regional peering and edge caching ecosystems closer to BharatNet aggregation points and district or block-level nodes.** Such localisation of traffic may significantly reduce rural bandwidth costs, improve latency, reduce upstream transit dependence and **strengthen long-term viability of rural Public Wi-Fi deployments.**

D5. Leveraging existing fibre and digital infrastructure of non-telecom entities

A strategic opportunity for accelerating Public Wi-Fi proliferation in India may lie in more **effective utilisation of existing fibre and digital infrastructure assets already deployed by various public utilities, government agencies and non-traditional network operators.** India today possesses significant fibre infrastructure beyond conventional telecom operator networks. Such infrastructure includes fibre assets of entities such as Power Grid, RailTel, state electricity utilities, Smart City networks, municipal fibre systems, oil and gas utilities, public sector agencies and cable television and MSO networks. In many cases, these networks already reach important transport corridors, institutional nodes, semi-urban areas, district centres and local access points. Accordingly, **TRAI may consider examining whether a shared digital infrastructure approach may help accelerate Public Wi-Fi proliferation, particularly in underserved and difficult geographies where incremental fibre deployment costs may otherwise remain high.**

Such an approach need not imply unrestricted or mandatory sharing of all infrastructure. Many utility and government fibre networks support critical operational systems and may involve legitimate security, operational and resilience considerations. Accordingly, any sharing framework should remain technically feasible, security-compliant, commercially negotiated and operationally appropriate. However, wherever feasible, mechanisms such as dark fibre leasing, managed backhaul access, municipal fibre partnerships, utility corridor access, neutral-host infrastructure models and open-access fibre frameworks may significantly reduce deployment costs and improve geographic spread of Public Wi-Fi infrastructure.

The role of **cable television and local cable distribution ecosystems** may also merit examination. In many urban and semi-urban areas, cable, MSO and LCO networks already possess extensive last-mile infrastructure and local access presence. Subject to technical feasibility and commercial viability, **such networks may potentially support neighbourhood-level Public Wi-Fi expansion, managed hotspot deployment and local broadband aggregation models**. International experiences discussed in the CP also suggest that successful Public Wi-Fi ecosystems often rely upon integrated use of municipal fibre, utility infrastructure and public digital assets rather than depending exclusively upon standalone telecom deployments.

A carefully designed shared-infrastructure approach may therefore help reduce duplication of civil infrastructure, accelerate hotspot deployment timelines, improve economics in remote and underserved areas, strengthen municipal and local participation and improve overall broadband efficiency. At the same time, appropriate safeguards relating to cybersecurity, network segregation, resilience, operational continuity and commercial fairness would remain essential.

D6. Active participation of municipalities and local bodies

The sixth strategic step should be **active participation of municipalities and local bodies.** Municipalities should not be viewed merely as permission-granting authorities. They should be **treated as local digital infrastructure coordinators**. **Their role may include identifying hotspot locations, providing access to street furniture, enabling fibre routes, rationalising rentals and Right of Way charges, coordinating with market associations, allowing use of public buildings, integrating Wi-Fi with smart-city assets and facilitating local public-private partnership models.**

D7. Differentiated deployment models for different geographies

The seventh strategic step should be to create differentiated models for different geographies. In dense urban and commercial zones, deployment may largely be market-led through ISPs, PDOAs, venue owners and commercial establishments. In high-footfall public locations, venue-led or public-private partnership models may be appropriate. In rural and remote areas, viability-gap support, BharatNet integration and anchor institution models may

be required. In tourist and heritage locations, tourism departments and local bodies may support hotspot deployment as part of visitor infrastructure.

D8. Execution roadmap rather than numerical targets alone

The eighth strategic step should be to develop a practical execution roadmap rather than merely numerical hotspot targets. India's experience shows that numerical targets alone may not ensure meaningful coverage, usage or sustainability. **A roadmap should focus on action sequencing, first mapping locations and infrastructure, then creating hotspot clusters, then enabling public infrastructure access, then improving authentication and roaming, and finally integrating Public Wi-Fi with local digital services.**

D9. Local demand aggregation

The ninth strategic step should be local demand aggregation. In many areas, a **single hotspot may not be viable, but a cluster of institutions, shops, public offices and community locations may create sufficient aggregated demand.** Local bodies, trade associations, market associations and Panchayats can play an important role in aggregating such demand and inviting ISPs, PDOAs and system integrators to deploy managed Public Wi-Fi networks.

D10. Making public-facing infrastructure Wi-Fi ready

The tenth strategic step should be making public-facing infrastructure Wi-Fi ready. **Large public buildings, transport hubs, markets, campuses, hospitals, tourist locations and municipal facilities should be encouraged to provide basic infrastructure readiness such as fibre access, power, mounting space and provider-neutral access.** This need not mean that every site must itself operate Wi-Fi, but it should be ready for service providers to deploy it quickly.

D11. District-level and city-level Public Wi-Fi plans

The other strategic step should be **development of district-level and city-level Public Wi-Fi plans.** These plans may identify priority hotspot clusters, underserved areas, available fibre, municipal assets, likely business models and responsible agencies. Such plans may be periodically updated and aligned with BharatNet, Smart Cities, state broadband policies and local digital governance programmes.

Public Wi-Fi proliferation should follow a spatially planned, locally coordinated and commercially differentiated strategy. The objective should not merely be to increase hotspot numbers, but to create useful, discoverable, dense and geographically inclusive Public Wi-Fi clusters across markets, institutions, transport systems, public places and underserved communities.

Such an approach would align with the CP's broader recognition that Public Wi-Fi can serve as a scalable and affordable access layer for broadband proliferation, digital inclusion, public service delivery and broader digital transformation.

Q4. What changes, if any, are required in the existing PM-WANI framework to improve revenue certainty and long-term sustainability for PDOs/PDOAs? Please provide your response in detail with justification.

A. THE PM-WANI FRAMEWORK: STRENGTHS TO BE PRESERVED

At the outset, it is important to recognise that the **PM-WANI framework represents a significant deregulatory and decentralised reform in India's broadband policy architecture. Its core strength lies in lowering entry barriers and enabling local participation in broadband access provisioning without requiring traditional telecom licensing structures.** The framework has enabled ordinary shops, institutions, public establishments and local entrepreneurs to potentially become part of India's digital connectivity ecosystem **through a people-to-people and business-to-community broadband access model.**

This decentralised philosophy is itself one of the most important strengths of PM-WANI and should be preserved. Any future policy evolution should therefore avoid reversing, diluting or re-centralising the light-touch structure already created. Regulatory stability and continuity are important for investor confidence, ecosystem trust and long-term innovation. **The objective should not be to re-regulate PM-WANI, but to build scalable aggregation, interoperability, innovation and commercial sustainability layers over the deregulated foundation already established.**

B. THE CORE CHALLENGE: FRAGMENTATION AND THE NEED FOR AGGREGATION

The principal challenge at present is not the conceptual viability of PM-WANI, but the absence of sufficient ecosystem scale and aggregation. The PDO layer will naturally remain fragmented and localised because the PDO is essentially a neighbourhood level participant, i.e. a shopkeeper, cafe owner, public venue, institution or local entrepreneur. Such fragmentation is not a weakness. Rather, it reflects the decentralised design philosophy of PM-WANI.

However, fragmented PDOs alone cannot create a scalable nationwide Public Wi-Fi ecosystem. **For scale, continuity, discoverability, user trust, interoperability and monetisation to emerge, the ecosystem requires stronger aggregation and platform layers. In this context, PDOAs and App Providers become strategically important. They should not be viewed merely as backend compliance or authentication entities. They have the potential to evolve into scalable digital connectivity platforms capable**

of aggregating large numbers of PDOs and creating a seamless user ecosystem. Their role can be analogous to digital aggregation platforms in other sectors, where fragmented local participants are connected into larger interoperable and trusted networks.

Accordingly, the long-term sustainability of PM-WANI may depend significantly upon **emergence of scalable PDOA ecosystems**, **innovative App Providers, interoperable roaming systems and platform-led service innovation**. The framework may therefore evolve in a manner that encourages aggregation, interoperability and innovation while preserving the decentralised participation model at the PDO level.

C. REQUIREMENTS FOR IMPROVING REVENUE CERTAINTY AND LONG-TERM SUSTAINABILITY

C1. Stronger aggregation and discovery ecosystems

The first requirement for improving sustainability is **development of stronger aggregation and discovery ecosystems.** Individual PDOs may not independently possess the scale required for marketing, customer acquisition, roaming integration, digital payments, analytics, customer support, loyalty systems or platform innovation. However, **scaled PDOAs and App Providers can aggregate thousands of PDOs into recognisable service ecosystems capable of creating user trust and continuity.** Such platforms may provide hotspot discovery, integrated onboarding, wallet systems, roaming packs, subscription models, multilingual interfaces, loyalty programmes, digital coupons, local commerce integration, customer analytics and user engagement systems. This may significantly improve the commercial attractiveness of Public Wi-Fi for both end users and local establishments.

C2. Diversification of revenue streams

The second requirement is diversification of revenue streams. Long-term sustainability of Public Wi-Fi ecosystems cannot depend solely upon sale of prepaid data sachets or hotspot-specific vouchers. While such models are useful during the early and localised stages of deployment, scalable ecosystems typically evolve toward **multiple coexisting monetisation models**. Accordingly, the **PM-WANI ecosystem may naturally evolve to support coexistence of prepaid sachets, subscriptions, wallet-based access, freemium models, advertising-supported access, venue-sponsored Wi-Fi, retail-bundled access, enterprise Wi-Fi, tourism-linked access, public-service connectivity**

Different models may emerge in different geographies and environments depending upon local economics and user behaviour. For example, retail establishments may derive value through increased customer footfall and digital visibility, transport hubs may support sponsored or freemium access, educational campuses may support institutional models, tourism locations may integrate Wi-Fi into visitor services, and enterprise environments may

support managed subscription models. **The framework should, therefore, remain commercially flexible and technology neutral rather than tied to any single monetisation architecture.**

C3. Evolution of revenue architecture as interoperability and roaming expand

The third requirement is recognition that the revenue architecture of PM-WANI may naturally evolve as interoperability and roaming expand. At present, many deployments operate through local voucher-based models where the user purchases access from a PDO and revenues are subsequently shared with PDOAs and associated platform entities. Such models are appropriate in fragmented and localised ecosystems.

However, as Public Wi-Fi ecosystems evolve toward interoperable and roaming-enabled architectures, commercial models may progressively transition toward hybrid usage-based and platform-based settlement systems. In such scenarios, users may increasingly purchase connectivity through platform wallets, subscriptions, roaming packs or application-based access systems, and revenues may increasingly arise from usage settlement rather than only local voucher resale. This represents a natural market-led evolution of the ecosystem rather than a departure from the PM-WANI philosophy.

Accordingly, local voucher models and platform-based usage settlement models may coexist depending upon geography, scale and commercial strategy. Over time, scaled PDOAs and App Providers may evolve capabilities relating to authentication, usage accounting, roaming, billing, digital wallets, subscriptions, multi-party settlement and revenue distribution. **The regulatory framework need not prescribe rigid billing structures or settlement mechanisms. Instead, it may remain sufficiently flexible to support evolution of interoperable commercial architectures while ensuring transparency and fair participation of PDOs.**

C4. Interoperable roaming and service continuity

The fourth requirement is interoperable roaming and service continuity. Public Wi-Fi ecosystems become significantly more valuable when users experience continuity across multiple hotspots rather than isolated access points. Users are more likely to adopt and repeatedly use Public Wi-Fi services if a single account, application, wallet or roaming pack works across multiple hotspots and locations. Accordingly, interoperable roaming frameworks may gradually emerge through common APIs, federated authentication, backend settlement systems and platform interoperability arrangements. Initially, roaming may emerge among a limited number of scaled PDOAs and App Providers before broader ecosystem interoperability develops over time.

C5. Fair and transparent revenue participation for PDOs

The fifth requirement is fair and transparent revenue participation for PDOs. While platform aggregation is important, t**he local PDO remains the physical access anchor of the ecosystem and must remain commercially relevant.** The PDO provides physical premises, local customer interface, device hosting, electricity, venue access and local visibility. Therefore, s**ustainable growth requires that PDOs continue receiving fair and transparent participation in revenue flows as ecosystems scale.** Accordingly, transparent commercial arrangements and clearly disclosed revenue-sharing principles between PDOs, PDOAs and platform entities may improve confidence and reduce disputes.

C6. Reduction of upfront burden on PDOs

The sixth requirement is reduction of upfront burden on PDOs. Many small establishments may hesitate to participate because of uncertainty regarding device cost, maintenance, bandwidth charges and operational complexity. This may be addressed through managed-service deployment models such as leased devices, revenue-share hotspot kits, subscription-based deployment, managed maintenance and remote provisioning systems. Such models may reduce entry friction and accelerate participation.

C7. Stronger integration with ISPs and TSPs

The seventh requirement is stronger integration with ISPs and TSPs. PM-WANI should not be viewed as competing with mobile broadband. Rather, Public Wi-Fi should evolve as a complementary broadband access layer capable of traffic offload, indoor capacity enhancement, affordable high-volume access and high-density broadband support. **The Government and the Authority may accordingly persuade and encourage TSPs and ISPs to offer Public Wi-Fi services alongside fixed broadband.** ISPs and TSPs may therefore increasingly participate through managed hotspot partnerships, wholesale backhaul, neutral-host architectures and traffic offload arrangements. Such participation can create more stable and predictable revenue streams for ecosystem participants while simultaneously improving network efficiency and reducing congestion.

C8. Strengthening user trust and platform familiarity

The eighth requirement is strengthening user trust and platform familiarity. A detailed note on this is appended at Annexure-I which are clear recommendations from BIF in this regard which we request TRAI to consider along with DoT, MeitY & Cert-In for necessary implementation. Scaled App Providers and PDOAs may help build consumer confidence through consistent branding, quality assurance, security standards, seamless onboarding, roaming continuity and trusted user experiences. This is important because Public Wi-Fi adoption ultimately depends not merely on hotspot existence, but on whether users perceive the ecosystem as dependable and convenient.

C9. Encouraging interoperable competition rather than excessive centralisation

The ninth requirement is to encourage interoperable competition rather than excessive centralisation. The ecosystem should ideally evolve toward competing yet interoperable platform ecosystems rather than a monopolistic or excessively fragmented structure. **Emergence of a limited number of strong scalable ecosystem players is natural and desirable. Such interoperable competition may stimulate innovation, service quality, customer engagement, roaming arrangements and platform differentiation.**

D. PM-WANI AS AN OPEN DIGITAL CONNECTIVITY PLATFORM

PM-WANI should increasingly be **viewed not merely as a hotspot framework, but as an open digital connectivity platform ecosystem capable of supporting broadband inclusion, local entrepreneurship, digital public infrastructure, smart city integration, retail digitisation and future high-capacity broadband access.** The long-term sustainability of the ecosystem may therefore depend upon **preserving its decentralised and deregulated foundation while simultaneously enabling scalable aggregation, platform innovation, interoperable roaming and diversified commercial models to evolve organically over time.**

The broad direction of policy evolution may include preserving the light-touch and decentralised character of PM-WANI, encouraging emergence of scalable PDOAs and App Providers considering that serious investment requires scale visibility, enabling interoperable settlement frameworks capable of supporting large-scale ecosystem participants, supporting coexistence of multiple monetisation models, facilitating gradual evolution toward roaming and usage based settlement architectures, improving transparency and fair participation for PDOs, reducing entry friction for local establishments, strengthening ISP and TSP integration and promoting innovation-led ecosystem growth.

Such an approach would align public interest objectives of affordable and inclusive broadband access with long-term economic sustainability, investment confidence and scalable digital ecosystem development.

Q5 Are there any other challenges currently faced by PDOAs/PDOs? If yes, what changes can enhance the participation of entrepreneurs under the PM-WANI framework? Please provide your response in detail with justification.

A. THE NATURE OF CHALLENGES BEYOND COMMERCIAL SUSTAINABILITY

In addition to issues relating to commercial sustainability and ecosystem scale addressed in the response to the preceding question, PDOs and PDOAs continue to face several operational, behavioural, awareness related and ecosystem-participation challenges. At the outset, it is important to recognise that PM-WANI represents a fundamentally different model from conventional telecom provisioning. The framework attempts to democratise broadband access participation by enabling ordinary shops, institutions, public establishments and local entrepreneurs to become part of the digital connectivity ecosystem without requiring

traditional telecom licensing structures. However, many potential participants continue to perceive Public Wi-Fi deployment as a telecom-grade technical activity requiring specialised expertise, operational complexity and uncertain commercial returns. This perception itself has become an important participation barrier.

B. KEY CHALLENGES FACED BY PDOS AND PDOAS

B1. Lack of ecosystem familiarity and confidence

A major challenge is lack of ecosystem familiarity and confidence. A significant number of potential PDOs remain unaware that PM-WANI is intended to function as a light touch and low entry barrier ecosystem. Many small establishments continue perceiving hotspot deployment as technically difficult, operationally risky or commercially uncertain. Accordingly, **there is a need to progressively make PM-WANI participation operationally similar to elements of digital public infrastructure (DPI) or other familiar digital participation ecosystems such as accepting UPI payments or joining digital commerce platforms.** The objective should be to ensure that becoming a PDO is viewed as a simple digital business enablement activity rather than a telecom operation.

B2. Absence of sufficiently mature managed service ecosystems

A second major challenge is the absence of sufficiently mature managed service ecosystems. Most small establishments are not equipped to independently manage authentication systems, software upgrades, security compliance, troubleshooting, roaming integration or customer support. Therefore, **the long-term scalability of PM-WANI may depend significantly upon emergence of managed service architectures led by serious PDOAs, ISPs and platform providers.** Under such models, hotspot devices may be supplied pre-configured, whereby onboarding may be largely digital, software upgrades may be remote, authentication systems may be centrally managed and operational support may be platform-led. This may substantially reduce technical burden on local entrepreneurs.

Today, most of the FTTX ONTs already come with an in-built WiFi Access Point. By converting this inbuilt WiFi AP into a PMWANI Public WiFi AP through a PMWANI compatible SSID based firmware update, it could go a long way in boosting the number of PMWANI based Public WiFi hotspots all across the country and thereby help connect the unconnected and bridge the digital divide using Public WiFi. This may be possibly considered.

B3. Upfront cost sensitivity

Another important challenge is upfront cost sensitivity. Small establishments may hesitate to invest in devices, maintenance and broadband upgrades where revenue certainty is unclear. This may be addressed through commercially flexible deployment models such as leased hotspot devices, subscription-based deployment, revenue-sharing arrangements,

managed hotspot kits and bundled broadband-plus-Wi-Fi offerings. Such approaches may reduce entry friction and improve participation.

B4. Insufficient awareness and onboarding support

The e**cosystem also requires stronger awareness and onboarding support**. Participation may improve through coordinated ecosystem-building efforts involving PDOAs, ISPs, Common Service Centres, municipalities, local trade associations, tourism bodies, educational institutions and digital literacy platforms. A simplified digital onboarding ecosystem may additionally be developed through which prospective PDOs can identify nearby PDOAs and ISPs, compare service offerings, estimate deployment costs, understand revenue models and onboard electronically.

B5. Lack of standardisation and interoperability at the operational layer

Another important challenge is lack of standardisation and interoperability at the operational layer. Different onboarding systems, device configurations and operational practices increase friction and reduce scalability. Accordingly, interoperable plug-and-play hotspot ecosystems may significantly improve participation. Standardised PM-WANI-compliant hotspot devices capable of remote provisioning, automated software updates, integrated authentication, security compliance and roaming readiness may materially reduce operational complexity for PDOs. At the same time, standardisation should not evolve into excessive regulation or rigid technology prescriptions. The framework should remain sufficiently flexible to encourage innovation and platform competition.

B6. Limited local ecosystem integration

A further challenge is limited local ecosystem integration. Public Wi-Fi adoption is likely to improve where PDO participation becomes linked with local commerce, retail engagement, tourism, educational services, public services, digital payments and community connectivity ecosystems. PDOAs and App Providers may therefore play an important role in creating value-added ecosystems around hotspots rather than limiting the business model only to resale of small data vouchers.

B7. Regulatory confidence and policy continuity

Another important aspect is regulatory confidence and policy continuity. Since PM-WANI represents a deregulatory and decentralised reform, ecosystem confidence may weaken if the framework is perceived as unstable, excessively re-regulated or operationally uncertain. Long-term entrepreneurial participation therefore requires continued policy stability and predictable ecosystem evolution.

C. THE STRATEGIC ROLE OF PDOAS AND APP PROVIDERS IN DRIVING PARTICIPATION

The role of PDOAs and App Providers is particularly important in addressing these challenges. Scattered PDOAs may not independently create scalable ecosystems. However, **mature PDOAs and App Providers with sufficient scale and long-term vision can aggregate fragmented hotspots into trusted digital connectivity ecosystems** through branding, roaming, customer support, discovery systems, digital payments, analytics, platform innovation and user engagement. Accordingly, t**he ecosystem may benefit from emergence of competing yet interoperable platform ecosystems capable of driving awareness, adoption and innovation at scale. PDOAs and App Providers are strategic ecosystem-building layers, and the participation of serious, scaled players is therefore of considerable importance.**

Overall, the broad objective should be to make PM-WANI participation operationally simple, commercially flexible, technically manageable, digitally integrated and entrepreneur-friendly. The long-term success of PM-WANI may ultimately depend not merely on policy permission, but on whether participation becomes easy, trusted and economically meaningful for ordinary businesses and local establishments across the country.

Q6 Are there improvements needed in the Authentication, Authorization, Roaming, and Payment architecture of the PM-WANI Framework? Please share suggestions, if any. Please provide your response in detail with justification.

A. THE NEED FOR ARCHITECTURAL EVOLUTION

Yes. Improvements in the Authentication, Authorization, Roaming and Payment architecture may become increasingly important as the PM-WANI ecosystem evolves from fragmented hotspot deployments toward scalable and interoperable Public Wi-Fi ecosystems. At present, the architecture remains largely hotspot-centric and transaction-centric, whereas future large-scale Public Wi-Fi ecosystems may require evolution toward more seamless, identity-based and interoperable connectivity models.

The current onboarding experience in many cases still involves repeated OTP verification, captive portal redirection, hotspot-specific authentication, application downloads, voucher purchase flows and repeated re-authentication across locations. Such friction materially reduces user convenience and weakens adoption. Users today are accustomed to always-on and seamless connectivity experiences through mobile broadband ecosystems. Public Wi-Fi adoption may therefore remain limited unless onboarding and continuity become significantly simpler. The long-term objective should be gradual evolution toward nearly invisible and ambient authentication experiences while preserving lawful traceability, security and user consent requirements.

B. AUTHENTICATION AND AUTHORISATION: TOWARD SEAMLESS AND INCLUSIVE FRAMEWORKS

B1. Evolution toward persistent identity-based authentication

One possible direction could be phased migration toward interoperable and persistent identity-based authentication frameworks such as Passpoint/, OpenRoaming-type architectures, federated authentication systems and device-based trusted identity models. Under such systems, users may authenticate once and thereafter connect automatically to participating hotspots without repeated OTP or captive-portal interactions. Such architectures may significantly improve service continuity, user convenience, repeat usage and behavioural familiarity with Public Wi-Fi services. At the same time, evolution toward such systems may need to remain phased and proportionate considering India's diversity of deployments, device ecosystems and operator maturity levels.

B2. Preserving inclusion-oriented onboarding alongside advanced frameworks

While the long-term evolution of Public Wi-Fi ecosystems may progressively move toward seamless and persistent authentication frameworks such as Passpoint or interoperable roaming architectures, it is equally important that inclusion-oriented onboarding options continue to remain available during ecosystem evolution. Browser-based and captive-portal-based authentication mechanisms may therefore continue to serve an important role, particularly for first-time users, users with limited-storage devices, low-cost smartphones or digitally less-familiar populations. Accordingly, future authentication frameworks may benefit from a layered approach combining advanced seamless authentication models with simplified browser-based onboarding journeys so that ecosystem scalability and technological evolution do not inadvertently reduce digital inclusion.

C. ROAMING AND INTEROPERABILITY: FROM ISOLATED HOTSPOTS TO CONNECTED ECOSYSTEMS

An allied and important requirement is interoperable roaming. Public Wi-Fi ecosystems become significantly more useful when users experience continuity across multiple hotspots rather than isolated access islands. Accordingly, interoperable roaming frameworks may gradually evolve through common APIs, federated authentication systems, interoperable settlement architectures and backend integration among PDOAs and App Providers. Initially, roaming may emerge among a limited number of scaled PDOAs and App Providers before broader interoperability evolves organically over time.

Importantly, interoperability should preferably evolve through federated and open ecosystem models rather than centralised monopoly architecture. **Interoperable architectures supporting scalable ecosystem operators may create stronger innovation and consumer choice.** The ecosystem may also benefit from stronger API

standardisation, interoperable onboarding frameworks, common roaming standards and standardised backend integration approaches. Such standardisation may improve scalability and interoperability without imposing rigid technology mandates.

D. PAYMENT ARCHITECTURE: FROM VOUCHER MODELS TO INTEROPERABLE SETTLEMENT SYSTEMS

D1. Evolution of payment models as the ecosystem scales

Payment architecture may also require evolution as the ecosystem scales. At present, many deployments operate through local voucher or sachet models where users purchase hotspot-specific access. Such models are appropriate in localised and early-stage deployments. However, as roaming and interoperability increase, payment ecosystems may progressively evolve toward hybrid models involving digital wallets, subscriptions, roaming packs, integrated application billing, usage-based settlement, enterprise billing, bundled plans and UPI-linked micro-payments. Accordingly, future payment architecture may increasingly become identity-linked and usage-linked rather than only hotspot-linked.

D2. Backend settlement systems and multi-party revenue distribution

Backend settlement systems may therefore become important components of scalable Public Wi-Fi ecosystems. As users move across interoperable hotspots, revenues may need to be distributed among PDOs, PDOAs, App Providers and associated platform entities based upon actual usage and settlement arrangements. Such systems may evolve through interoperable clearing house architectures, federated settlement systems or platform-led settlement ecosystems where serious ecosystem operators will play a crucial role. Importantly, the framework should remain sufficiently flexible to support coexistence of local voucher-based access models and larger roaming-enabled platform ecosystems. Different commercial architectures may coexist depending upon geography, scale, user behaviour and business strategy.

E. SECURITY, TRUST AND COMPLIANCE

Security and trust considerations will also remain critical. Simplification of onboarding should not compromise cybersecurity, lawful traceability, user privacy or operational security. BIF wishes to highlight that the issue of Trust and Safety for Public Wi-Fi users is of considerable importance and urges the Authority to include appropriate recommendations to the Government to improve overall trust and safety and to address the negative publicity that sometimes flows from official communications cautioning users against Public Wi-Fi. BIF's detailed submissions on this subject are set out in Annexure -I and are not repeated here. Accordingly, future architectures may balance seamless onboarding, persistent identity, secure authentication, proportional compliance and transparent user consent mechanisms.

Overall, the long-term objective should be to enable PM-WANI to gradually evolve from fragmented hotspot-centric connectivity toward a seamless and interoperable digital connectivity ecosystem where authentication, roaming and payments become largely frictionless from the user's perspective while remaining secure, scalable and commercially sustainable in the background. The success of Public Wi-Fi adoption in India may ultimately depend not merely on hotspot availability, but on whether users experience Public Wi-Fi as a trusted, continuous and convenient extension of India's broader digital connectivity ecosystem.

Q7. In the Indian context, which of the following models would be more appropriate for the proliferation of Public Wi-Fi?

a. A model where the Government actively ensures hotspot deployment through direct funding and implementation support, including backhaul provision; or

b. A model where the Government primarily ensures availability of robust backhaul infrastructure and intervenes in hotspot deployment only in cases of market failure. Please provide your response in detail with justification.

A. FRAMING THE CHOICE: A TWO-LAYER ANALYTICAL APPROACH

In the Indian context, a mix of Government-led and market-led Public Wi-Fi ecosystem supported by strong enabling digital infrastructure and targeted public intervention may be more sustainable and scalable. Before selecting between the two options presented, it is important to distinguish between the broadband infrastructure layer and the retail hotspot service layer, as the nature of appropriate public and private participation differs significantly across these two layers.

The broadband infrastructure layer includes fiberisation, backhaul, ducts, utility corridors, public infrastructure access, municipal coordination, BharatNet connectivity and enabling digital infrastructure for Public Wi-Fi. The hotspot service layer includes hotspot deployment, user onboarding, roaming, customer engagement, platform innovation, monetisation models, authentication systems and service delivery.

targeted Government intervention is required particularly at the hotspot/access layer where commercial incentives remain insufficient or there are cases of market failure . This layered understanding is important because it allows the answer to avoid a binary choice between options (a) and (b) and instead recommend a calibrated and context-sensitive framework appropriate to India's conditions.

B. EVIDENCE OF MARKET FAILURE AND THE CASE FOR TARGETED PUBLIC SUPPORT

Though the CP brings out that successful international Public Wi-Fi ecosystems such as those in South Korea and the European Union evolved not merely through direct hotspot subsidies but through strong public investment in enabling infrastructure combined with local participation, municipal coordination, interoperable frameworks and scalable ecosystem development, Indian conditions are somewhat different and the same models may not exactly apply.

Given that Public Wi-Fi has been in existence for more than two decades based on the centralised ISP and TSP model, and thereafter for six years using the decentralised and unbundled PM-WANI model, the number of Public Wi-Fi hotspots generated so far in the country remains severely inadequate, thereby signifying a clear instance of market failure. This market failure cannot be attributed solely to policy design. It reflects a combination of ecosystem immaturity, awareness gaps, commercial misalignment, infrastructure deficits and the absence of sufficient aggregation and support mechanisms. A purely market-led approach has therefore demonstrably not produced the scale of Public Wi-Fi proliferation that India's digital ambitions require and to meet the Government's own ambitious targets of achieving 5 Mn PWHs by 2020, 10 Mn by 2022 (Ref: NDCP 2018) and 50 Mn PWHs by 2030 (Bharat 6G Vision document , 2023)

Accordingly, there is a clear need for Government intervention and State-supported funding and handholding, particularly at the infrastructure level and in rural, remote and underserved areas, to give this initiative the momentum it requires. However, it is equally important to recognise that subsidy or funding on its own cannot be the catalyst for all markets. Any assumption that financial support alone will drive adoption and scale across all geographies and commercial environments would be incorrect. The effectiveness of public support depends critically upon how it is targeted, what conditions it is attached to and whether it is designed to catalyse market participation rather than substitute for it.

C. THE PREFERRED FRAMEWORK: A BALANCED AND LAYERED APPROACH

Accordingly, a hybrid and layered framework broadly aligned with option (a) may be more appropriate for India, while retaining targeted intervention capabilities in areas of market failure and strategic public need. India's PM-WANI framework itself is based upon a decentralised and deregulated participation model. This is an important strength that should be preserved. The framework enables ordinary shops, institutions, public establishments and local entrepreneurs to participate in broadband access provisioning without requiring traditional telecom licensing structures. The preferred framework should build upon this foundation rather than replace it.

C1. Government's role at the infrastructure and enabling layer for Public Wi-Fi

At the infrastructure and enabling layer, Government's role may appropriately include accelerating fibreisation, strengthening BharatNet integration, enabling open-access backhaul, facilitating access to public infrastructure, simplifying Right of Way processes,

promoting interoperability frameworks, encouraging municipal participation, supporting public institutions and addressing inclusion gaps where commercial viability remains weak. Such enabling infrastructure investment coupled with Government led and Government supported hotspot creation in areas where there are demonstrable cases of market failure along with a blended mix of market-led hotspot deployment can scale effectively and sustainably.

C2. Targeted Government support at the hotspot layer in market-failure scenarios

At the hotspot service layer, direct Government led and Government supported deployment and funding will remain appropriate in specific scenarios involving remote and underserved regions, public health centres, Gram Panchayat facilities, disaster-prone areas, tourism zones and socially important public access locations where market incentives may initially remain insufficient. In rural areas, targeted support, including Government support for equipment procurement, operational costs and digital onboarding, may be provided to smaller PDOs to help them establish and operate their hotspots. This is notwithstanding the fact that even in such cases, a public private partnership oriented and infrastructure enabled approach could perhaps prove sustainable than fully supported hotspot operation models in the long run.

Government's role at the hotspot layer may therefore be characterised as strategic and catalytic rather than universal or operational. Funding and support mechanisms should be designed to reduce entry barriers and demonstration risk for local entrepreneurs, not to operate centralised hotspot networks in markets where commercial participation is feasible.

C3. Market-led participation at scale

A key consideration is that Public Wi-Fi ecosystems ultimately require continuous innovation, evolving commercial models, customer engagement, roaming ecosystems, seamless onboarding and scalable aggregation.. Such an approach may create a strong ecosystem enabling stakeholders such as PDOs, PDOAs, App Providers, ISPs, TSPs, local entrepreneurs and commercial establishments to build scalable Public Wi-Fi ecosystems. Public Wi-Fi adoption ultimately depends upon user trust, service continuity, quality, platform innovation and meaningful integration into daily digital usage patterns. Scalable ecosystems may emerge more effectively where commercial incentives, platform aggregation and local entrepreneurship are aligned, backed by targeted support especially in areas where there are market failures and also in rural and remote areas.

C4. Municipal and local body participation

Municipalities and local bodies may also play an important enabling role. International examples discussed in the CP demonstrate that local governments can significantly accelerate Public Wi-Fi proliferation through access to street furniture, municipal fibre systems, public buildings, Smart City infrastructure, local hotspot planning and simplified

permissions. Indian municipalities, Panchayats and local bodies may similarly function as local digital infrastructure facilitators rather than merely approval authorities.

Thus, a purely laissez-faire approach may be insufficient given India's geographic diversity and digital inclusion objectives. Equally, a purely Government directed model risks substituting for market innovation rather than catalysing it. The preferred framework for India may therefore be characterised as a mix of Government funded and Government supported intervention, especially in rural and remote areas and in cases of market failure, alongside market-scaled, locally coordinated and inclusion-sensitive ecosystem development. Government should strengthen enabling digital infrastructure and address market failures, Each State Government through State Broadband Committees should be encouraged to include PWH targets as part of the National Target laid down in the Bharat 6G Vision and form a task force to ensure its time bound implementation. Municipalities should facilitate local execution by enabling and encouraging local deployment of PWHs under each of their wards through a mission mode project-on the lines of RoW; and market participants should drive hotspot proliferation, innovation, aggregation and user adoption.

This balanced approach may best align public interest objectives, digital inclusion goals, investment efficiency, innovation incentives and long-term ecosystem sustainability. Over time, such a model may allow Public Wi-Fi in India to evolve not merely as isolated hotspot deployment, but as an integrated and scalable broadband access layer supporting India's broader digital economy and connectivity objectives.

Q8. Is there a need to adopt separate strategies for Public Wi-Fi proliferation in rural and urban areas? If yes, suggestions may be provided. Please provide your response in detail with justification.

A. **WHY DIFFERENTIATED STRATEGIES ARE NECESSARY**

Yes. Separate and differentiated strategies may be necessary for Public Wi-Fi proliferation in rural and urban areas because the underlying economics, infrastructure conditions, usage patterns, institutional ecosystems and connectivity objectives differ substantially across these environments. It is important to recognise at the outset that Public Wi-Fi performs different functional roles in rural and urban ecosystems.

In urban environments, Public Wi-Fi primarily functions as a density augmentation layer, a high-capacity broadband access layer, a traffic offload mechanism and an indoor connectivity enhancement ecosystem. In rural and underserved environments, Public Wi-Fi may function more as a digital inclusion mechanism, a shared community access layer, a last-mile broadband extension architecture and a public-service connectivity platform.

State governments may encourage PM-WANI deployment in government institutions, supported by BharatNet connectivity and integrated with digital governance and educational use-cases.

Urban building bye-laws should incorporate telecom and in-building digital infrastructure provisions to improve indoor broadband and Wi-Fi deployment.

Accordingly, a uniform national deployment model may not be appropriate. Urban and rural Public Wi-Fi ecosystems may therefore require differentiated, though interoperable, strategies aligned with local infrastructure realities, user behaviour and commercial viability conditions.

B. URBAN PUBLIC WI-FI STRATEGY: DENSITY, PLATFORMS AND COMMERCIAL ECOSYSTEMS

B1. Characteristics and strategic focus

In urban areas, Public Wi-Fi proliferation may largely evolve through commercially driven and platform-led ecosystems. Urban environments typically possess higher fibre density, stronger broadband backhaul, higher smartphone penetration, concentrated footfall, greater commercial activity and stronger monetisation potential. Accordingly, urban Public Wi-Fi ecosystems may scale through adoption by commercial establishments, transport hubs, educational campuses, hospitals, tourism zones, public spaces, markets and high-density commercial clusters. The urban strategy may therefore focus primarily upon hotspot density, continuity, roaming, seamless onboarding and platform aggregation.

B2. Wi-Fi zones, corridors and institutional ecosystems

Rather than isolated hotspots, emphasis may be placed upon creation of Wi-Fi zones, hotspot clusters, transport corridors, tourism circuits, commercial districts and institutional connectivity ecosystems. Municipalities and urban local bodies may play an important enabling role in facilitating hotspot location access, simplifying permissions and coordinating with local infrastructure. Urban building bye-laws should additionally incorporate telecom and in-building digital infrastructure provisions to improve indoor broadband and Wi-Fi deployment. Urban Public Wi-Fi may also increasingly integrate with traffic offload arrangements, retail engagement systems, local commerce, tourism services and digital public infrastructure platforms.

B3. Platform-led aggregation in urban environments

Platform-led ecosystems involving PDOAs and App Providers may become especially important in urban environments because they can provide aggregation, roaming, authentication continuity, discovery, digital payments, customer engagement and service innovation at scale.

C. RURAL PUBLIC WI-FI STRATEGY: INCLUSION, INSTITUTIONAL ANCHORS AND GRADUAL ECOSYSTEM DEVELOPMENT

C1. Structural differences and strategic objectives

In contrast, rural Public Wi-Fi proliferation may require a different strategic approach because rural connectivity economics are structurally different. Rural areas often face lower population density, weaker commercial viability, lower purchasing power, sparse institutional infrastructure, limited fibre reach and lower traffic concentration. Accordingly, the primary objective in rural areas may initially be meaningful access and inclusion rather than dense commercial hotspot ecosystems.

C2. BharatNet as the foundational rural backhaul layer

In this context, BharatNet may play a foundational role as the enabling rural backhaul infrastructure for Public Wi-Fi proliferation. BharatNet-connected Gram Panchayats and public institutions may function as anchor connectivity nodes around which local Public Wi-Fi ecosystems can gradually evolve. State governments may additionally encourage PM-WANI deployment in government institutions, supported by BharatNet connectivity and integrated with digital governance and educational use-cases. Accordingly, rural strategies may focus upon community access, institutional access, shared connectivity models and public-service integration.

C3. Local institutional participation and community anchors

Panchayats and district administrations may also play an important facilitative role through local infrastructure coordination, identification of public locations, community awareness, integration with local development programmes and aggregation of local demand. Unlike urban ecosystems, rural Public Wi-Fi models may initially depend more upon shared community access, institutional usage, educational access, e-governance services, telemedicine, digital agriculture and public digital service delivery.

C4. Commercial models and public support in rural areas

Commercial models in rural areas may, therefore, evolve differently. Targeted public support and viability-gap intervention may also be justified in remote and underserved regions where market incentives alone may not initially support deployment. However, the long-term objective should remain gradual ecosystem sustainability rather than permanent subsidy dependence. Public intervention may, therefore, function primarily as ecosystem catalysation and inclusion support, while allowing local entrepreneurship and market participation to evolve progressively over time.

D. DIFFERENTIAL PACE OF EVOLUTION AND THE IMPORTANCE OF INTEROPERABILITY

Another important consideration is that rural and urban ecosystems may evolve at different speeds and through different technological pathways. Urban ecosystems may rapidly adopt

roaming, subscriptions, platform-based access and seamless authentication systems. Rural ecosystems may initially continue using simpler onboarding systems, community-level access and locally managed usage models. Accordingly, the framework should remain sufficiently flexible to accommodate multiple commercial and operational models simultaneously.

At the same time, interoperability between rural and urban ecosystems should remain an important long-term objective so that users experience Public Wi-Fi as part of a unified national digital connectivity ecosystem. International experiences discussed in the CP also suggest that successful Public Wi-Fi proliferation generally depends upon adapting deployment models to local realities rather than imposing uniform national architectures.

Thus, the preferred approach for India may involve differentiated deployment strategies, common interoperability principles, strong enabling infrastructure, local institutional participation, platform-led innovation and geographically appropriate business models. Urban Public Wi-Fi strategies may focus primarily upon density, capacity augmentation, roaming, commercial ecosystems and platform scalability, while rural Public Wi-Fi strategies may focus primarily upon inclusion, shared access, institutional anchors, BharatNet integration and gradual ecosystem development. Such differentiated yet interoperable strategies may better align with India's geographic diversity, digital inclusion objectives and long-term broadband growth requirements.

Q9. What measures can be taken to improve the deployment and uptake of Public Wi-Fi networks in high-footfall areas for both outdoor (such as bus stops, roadside transit points, open public parks, markets, tourist sites), and indoor (such as airports, railway stations, malls, public institutions)? Please provide your response in detail with justification, separately for outdoor and indoor scenarios.

A. HIGH-FOOTFALL AREAS AS STRATEGIC ANCHORS FOR PUBLIC WI-FI ADOPTION

High-footfall areas may represent one of the most important strategic opportunities for large-scale Public Wi-Fi proliferation in India, especially in metros and Tier-1 cities, because they combine concentrated user demand, repeat usage patterns, higher visibility, stronger monetisation potential and natural opportunities for behavioural adoption of Public Wi-Fi services. Such locations may therefore function as anchor ecosystems through which Public Wi-Fi becomes a visible, trusted and habitually used component of India's digital connectivity architecture.

At the same time, outdoor and indoor Public Wi-Fi environments differ substantially in terms of infrastructure characteristics, deployment economics, ownership structures, user behaviour and operational requirements. Accordingly, separate but interoperable strategies may be appropriate for outdoor and indoor scenarios.

B. OUTDOOR PUBLIC WI-FI: DEPLOYMENT MEASURES AND STRATEGIES

B1. Characteristics of outdoor environments and the case for clustered deployment

Outdoor Public Wi-Fi environments such as bus stops, roadside transit points, markets, tourist sites, public parks and public gathering areas primarily require spatial continuity, wide-area coverage, public infrastructure integration and cost-efficient deployment architectures. In such environments, isolated hotspot deployment may not create sufficient user value. Instead, deployment strategies may focus on creation of Wi-Fi corridors, hotspot clusters, market zones, transport connectivity zones, tourism circuits and digitally connected public spaces. Such clustered deployment may significantly improve discoverability, repeat usage and user familiarity.

B2. Municipal and local body participation

Municipalities and urban local bodies may play an especially important enabling role in outdoor deployments by facilitating access to street furniture, smart poles, bus shelters, public buildings, traffic infrastructure, municipal fibre, public power access and Smart City infrastructure. Many cities already possess fibre-connected smart infrastructure created under Smart City and urban surveillance programmes. Public Wi-Fi deployment may often be integrated with such infrastructure at comparatively lower incremental cost. Simplified municipal permissions, standardised infrastructure access frameworks and coordinated local deployment policies may significantly accelerate rollout in outdoor public spaces.

B3. Shared infrastructure, commercial models and digital service integration

Shared and neutral host infrastructure models may also improve deployment efficiency by reducing duplication of equipment and civil infrastructure. Depending upon geography and footfall characteristics, outdoor Public Wi-Fi ecosystems may support multiple commercial models including freemium access, advertising-supported access, tourism-linked services, retail-integrated access, public service connectivity and local commerce engagement. Outdoor Public Wi-Fi may additionally support digital tourism services, navigation, local information systems, emergency alerts, multilingual assistance, transport information and civic communication systems. Such integration may materially improve both utility and sustainability. Mesh-based and centrally managed hotspot architectures may also improve scalability in outdoor deployments, particularly in dense public areas and transit corridors.

C. INDOOR PUBLIC WI-FI: DEPLOYMENT MEASURES AND STRATEGIES

C1. Characteristics of indoor environments and infrastructure expectations

For indoor environments such as airports, railway stations, metro systems, malls, hospitals, educational campuses, public institutions, convention centres and large commercial

buildings, Public Wi-Fi may progressively evolve into a standard digital infrastructure expectation similar to broadband readiness or utility connectivity. Indoor environments generally involve high user density, heavy indoor data usage, longer dwell times, high quality connectivity expectations and significant mobile network congestion. Accordingly, indoor Public Wi-Fi systems may increasingly evolve toward managed high-capacity broadband environments integrated with venue infrastructure.

C2. Wi-Fi readiness, venue flexibility and provider neutrality

Large venues may therefore be encouraged to maintain Public Wi-Fi readiness through fibre availability, structured cabling, power access, provider-neutral infrastructure, mounting space and managed deployment capability. At the same time, venue owners should retain flexibility to procure services from any authorised ISP or PDOA. Such flexibility may improve competition, innovation and service quality. Indoor Public Wi-Fi systems may additionally support mobile traffic offload, digital ticketing, venue navigation, retail engagement, customer analytics, digital advertising, enterprise applications, public information systems and integrated digital service ecosystems.

C3. Seamless onboarding, roaming and advanced authentication frameworks

Seamless onboarding and roaming may be especially important in indoor environments because users increasingly expect frictionless connectivity experiences comparable to mobile broadband. Accordingly, gradual migration toward persistent authentication, interoperable roaming and platform-based onboarding may materially improve adoption and repeat usage. High-footfall indoor environments may also become important demonstration zones for advanced Public Wi-Fi ecosystems involving Passpoint and OpenRoaming architectures, integrated digital wallets, venue-linked digital services and interoperable platform ecosystems.

D. BEHAVIOURAL ROLE OF HIGH-FOOTFALL AREAS AND PREFERRED POLICY APPROACH

Another important consideration is that high-footfall areas may play a critical behavioural role in mainstreaming Public Wi-Fi usage in India. Users are more likely to trust and habitually use Public Wi-Fi when they encounter reliable connectivity, consistent branding, visible deployment and seamless experiences in major public environments such as transport systems, commercial districts, educational institutions and public venues. Accordingly, high-footfall environments may become the **initial large-scale adoption anchors from which broader Public Wi-Fi familiarity and ecosystem growth can progressively spread.**

From a policy perspective, the preferred approach may therefore involve strong municipal and venue-level participation, integration with public digital infrastructure, provider-neutral deployment frameworks, platform-led service innovation, interoperable roaming evolution

and commercially flexible business models. Such an approach may enable ***high-footfall areas*** *to function not merely as isolated hotspot locations, but* ***as visible and scalable Public Wi-Fi ecosystems supporting India's broader digital connectivity, public-service and broadband inclusion objectives****.*

Q10. If the Government decides to provide financial support for the proliferation of Public Wi-Fi, which funding mechanisms would be most suitable for India? Should a uniform funding mechanism be adopted nationwide, or should differentiated funding mechanisms be used for rural, urban, and high- footfall areas? Please provide your response in detail with justification.

A. THE CASE FOR A TARGETED, CATALYTIC AND DIFFERENTIATED FUNDING FRAMEWORK

As mentioned earlier in response to Q7, Government support maybe considered necessary for accelerating Public Wi-Fi proliferation in targeted areas in the urban locales where there are demonstratable cases of market failure, besides targeted funding support for setting up hotspots access in the rural and remote areas. ,

The preferred approach may be a targeted, catalytic and differentiated funding framework rather than a uniform nationwide subsidy model. It is important to recognise that Public Wi-Fi ecosystems across India differ substantially in terms of infrastructure availability, population density, commercial viability, user behaviour, institutional participation and digital inclusion requirements. Accordingly, a single uniform funding mechanism may neither be economically efficient nor operationally appropriate.

The fundamental objective of public funding should be to address market failure, reduce ecosystem entry barriers, strengthen enabling infrastructure, support inclusion and catalyse sustainable ecosystem development. The effectiveness of public funding depends critically upon how it is targeted, what conditions it is attached to and it should be designed to catalyse the market growth. Different categories of geographies may therefore require different funding approaches.

B. FUNDING APPROACH FOR RURAL AND UNDERSERVED AREAS

In rural and underserved regions, commercial viability may initially remain weak because of lower population density, lower purchasing power, sparse commercial ecosystems and limited infrastructure availability. Accordingly, funding in such regions may focus primarily upon supporting small entrepreneurs, Village Level Entrepreneurs and MSMEs in setting up hotspots and sustaining them through the initial years until they become self-sufficient. Alongside such entrepreneur support, funding may also extend to institutional anchor connectivity, shared community access models, infrastructure grants and public-service integration.

Public institutions such as Gram Panchayat offices, schools, colleges, Primary Health Centres, Common Service Centres and rural service centres may function as anchor nodes for rural Public Wi-Fi proliferation. In such environments, public support may act as an ecosystem catalyst until sufficient local usage and entrepreneurship gradually emerge.

C. FUNDING APPROACH FOR URBAN AREAS

In urban areas, Public Wi-Fi ecosystems may often become commercially viable through commercial establishments, transport systems, retail ecosystems, tourism and platform aggregation. Accordingly, direct operational subsidies may generally be less necessary in commercially viable urban environments. Instead, public intervention in urban areas may focus primarily upon municipal infrastructure access, simplified permissions, Smart City integration, public infrastructure readiness, fibre corridors, access to poles and street furniture and support for interoperable public digital infrastructure. Such enabling measures may significantly reduce deployment costs while preserving market-led innovation and competition.

D. FUNDING APPROACH FOR HIGH-FOOTFALL AREAS

For high-footfall areas such as railway stations, airports, bus terminals, tourism circuits, markets, educational campuses and public institutions, PPP-oriented models, venue partnerships and shared infrastructure approaches may be more appropriate. These environments often possess concentrated demand, stronger monetisation potential, advertising opportunities and integrated digital-service ecosystems. Accordingly, sustainable funding structures in such areas may increasingly evolve through venue-led models, advertising-supported ecosystems, managed service arrangements and integrated digital engagement platforms.

E. DESIGN PRINCIPLES FOR FUNDING MECHANISMS

Funding mechanisms may therefore be designed in a manner that reduces initial deployment friction, strengthens enabling infrastructure, supports inclusion objectives and gradually encourages market-led sustainability over time. Different mechanisms such as viability gap funding, infrastructure grants, PPP frameworks, public infrastructure sharing, institutional connectivity support, outcome-linked support and ecosystem development incentives may coexist depending upon geography and deployment context.

Overall, the preferred approach for India may therefore be differentiated rather than uniform across all regions, and catalytic rather than subsidy driven. Public funding should be calibrated to the commercial and infrastructure conditions of each geography, targeted toward reducing market failure and entry barriers, and structured to enable market-led participation to emerge and sustain itself progressively over time.

Q11. What criteria should govern the allocation and disbursement of funds across rural, urban, and high-footfall areas respectively? Please provide your response in detail with justification.

A. GUIDING PRINCIPLES FOR FUND ALLOCATION AND DISBURSEMENT

The allocation and disbursement of Public Wi-Fi funding may be guided by principles of catalysation, inclusion, sustainability, infrastructure efficiency, public utility and long-term ecosystem viability. Funding disbursement criteria may focus not only upon deployment numbers, but also upon actual usage potential, public-service value, ecosystem sustainability and long-term operational viability. Different criteria may appropriately apply across rural, urban and high-footfall environments.

B. GEOGRAPHY-SPECIFIC ALLOCATION CRITERIA

B1. Rural and underserved areas

In rural and underserved areas, allocation criteria may prioritise absence or inadequacy of broadband access, digital inclusion requirements, remoteness, institutional importance, educational and healthcare relevance, BharatNet availability and community-level impact. Priority may be accorded to locations where Public Wi-Fi can materially improve access to education, telemedicine, e-governance, digital payments, agriculture services and public digital infrastructure. The presence of anchor institutions such as Gram Panchayats, schools, Common Service Centres, Primary Health Centres and public service centres may also be considered important because such institutions can improve both utilisation and sustainability.

B2. Urban areas

In urban environments, criteria may focus more upon population density, footfall concentration, public space utility, fibre readiness, municipal participation and infrastructure sharing potential. Priority may be accorded to transport hubs, public markets, commercial districts, educational campuses, tourism zones, dense public-use environments and Smart City ecosystems.

B3. High-footfall areas

In high-footfall environments, allocation may additionally consider expected user volumes, duration of user presence, tourism importance, transport integration, enterprise usage potential and opportunities for digital public-service integration.

C. ALLOCATION AND DISBURSEMENT CRITERIA

C1. Infrastructure readiness and inclusion balance

Another important criterion may be infrastructure readiness. Locations where affordable fibre backhaul, power supply, public infrastructure access and institutional coordination already exist may enable faster and more cost-efficient deployment. At the same time, allocation frameworks should avoid favouring only easy-to-serve locations at the expense of underserved regions. Accordingly, a balance may be maintained between inclusion impact and deployment efficiency.

C2. Local participation and sustainability commitment

Funding frameworks may also consider local participation and sustainability commitment. Municipalities, Panchayats, institutions, PDOAs and local ecosystem participants may be encouraged to contribute through infrastructure access, co-funding, local coordination, maintenance support or demand aggregation. Such participation may improve accountability and long-term sustainability.

C3. Performance-linked and sustainability-linked disbursement

Disbursement mechanisms may additionally evolve toward performance-linked and sustainability-linked approaches. Rather than one-time deployment-linked funding alone, disbursement may progressively consider operational uptime, active usage, quality of service, continuity of operation, public-service integration and user adoption levels. This may improve long-term effectiveness and reduce risk of inactive or unsustainable deployments. At the same time, compliance and reporting obligations should remain proportionate, particularly for smaller PDOs and local entrepreneurs.

The overall objective should therefore be to create a funding framework that promotes meaningful and inclusive broadband access, encourages sustainable ecosystem development, supports efficient utilisation of public resources and catalyses long-term market-led Public Wi-Fi proliferation across diverse Indian geographies.

Q12. Is the lack of adequate and reliable last-mile connectivity a critical constraint for the proliferation of Public Wi-Fi in the country? If yes, what specific measures may be considered by the Central Government, State Governments, and local bodies to address the last-mile constraints? Please provide your response in detail with justification.

A. **LAST MILE CONNECTIVITY AS A FOUNDATIONAL CONSTRAINT**

Yes. Adequate, reliable and affordable last mile connectivity remains one of the most critical foundational constraints affecting large-scale proliferation of Public Wi-Fi in India. It is

important to recognise at the outset that Public Wi-Fi ecosystems are fundamentally dependent upon the quality and resilience of underlying broadband infrastructure. A hotspot can deliver meaningful broadband access only if supported by reliable last-mile and backhaul connectivity. Accordingly, Public Wi-Fi proliferation cannot be viewed in isolation from broader national fibreisation and digital infrastructure strategies.

The issue becomes particularly important in rural and underserved regions, dense urban areas with insufficient fibreisation, high-footfall environments, indoor congestion zones and geographically difficult areas. It may also be useful to distinguish between middle mile connectivity and last mile connectivity. While initiatives such as BharatNet have significantly improved middle mile reach in many parts of the country, the challenge of economically viable local last-mile distribution often continues to persist. In many cases, fibre may reach a Gram Panchayat or institutional node, but affordable and scalable extension from the aggregation point to local hotspots, public spaces, commercial establishments or community access locations may remain inadequate. Accordingly, Public Wi-Fi proliferation should be closely integrated with broader national fibreisation and shared digital infrastructure strategies.

B. MEASURES BY THE CENTRAL GOVERNMENT

B1. Enabling infrastructure frameworks and fibreisation

The Central Government may play an important role in strengthening enabling infrastructure frameworks through accelerated fibreisation policies, promotion of open-access and shared digital infrastructure models, integration of BharatNet with Public Wi-Fi ecosystems, common duct and utility corridor policies, facilitation of interoperable backhaul access, support for neutral-host infrastructure and encouragement of infrastructure sharing frameworks.

B2. Leveraging non-traditional fibre assets

An additional strategic opportunity may lie in more effective utilisation of existing fibre assets deployed by public utilities, government agencies and non-traditional infrastructure entities. India today possesses significant fibre infrastructure beyond conventional telecom operator networks, including assets associated with PowerGrid, RailTel, state electricity utilities, Smart City networks, municipal fibre systems, public sector infrastructure agencies and cable television and MSO ecosystems. Where technically feasible, commercially viable and operationally appropriate, such infrastructure may help accelerate Public Wi-Fi backhaul availability, particularly in underserved and difficult geographies.

B3. BharatNet integration and rural broadband deepening

The long-term success of rural Public Wi-Fi proliferation may depend significantly upon deeper operational integration between BharatNet and PM-WANI ecosystems. BharatNet

may progressively evolve not merely as a fibre deployment initiative, but as an active and open-access rural broadband distribution backbone capable of supporting scalable last-mile Public Wi-Fi ecosystems. In this regard, transparent wholesale access frameworks, defined service-level standards, uptime accountability and simplified access arrangements for licensed ISPs may materially improve utilisation of BharatNet infrastructure. Simultaneously, India may benefit from gradual extension of regional peering and edge caching ecosystems closer to BharatNet aggregation points and district or block-level nodes. Such localisation of traffic may significantly reduce rural bandwidth costs, improve latency, reduce upstream transit dependence and strengthen long-term viability of rural Public Wi-Fi deployments.

B4. The BharatNet Udyami model as a convergence mechanism between BharatNet and PM-WANI

An operationally important mechanism that the Central Government may consider strengthening in this context is the BharatNet Udyami model. The BNU framework enables local entrepreneurs to extend BharatNet connectivity from Gram Panchayat aggregation points to surrounding villages, habitations and community locations, functioning as local last-mile distribution operators. The CP notes that local bodies can facilitate and encourage participation in the BNU model as a means of extending rural broadband reach.

BIF submits that there is a significant and under explored convergence opportunity between the BNU model and the PM-WANI PDO and PDOA framework. A BharatNet Udyami operating as a last-mile broadband distributor is structurally well positioned to simultaneously function as a PDOA or managed hotspot operator, extending both individual broadband connections and Public Wi-Fi access to surrounding communities from the same BharatNet-anchored infrastructure. Aligning the BNU framework with PM-WANI operational requirements, through simplified dual registration, shared compliance frameworks, combined onboarding processes and coordinated technical support, may significantly reduce the cost and complexity of rural Public Wi-Fi deployment while improving the commercial sustainability of BNU operations through additional revenue from hotspot services.

The Authority may therefore consider recommending to the Government that the BNU and PM-WANI frameworks be formally aligned to enable and encourage BNUs to participate as managed hotspot operators, with appropriate technical, operational and commercial support to facilitate this dual role.

B5. Shared infrastructure and neutral-host models

Another important requirement is promotion of shared infrastructure and neutral-host approaches. Duplication of fibre, poles and access infrastructure may significantly increase deployment costs and reduce viability, especially in low-density geographies. Shared infrastructure models may therefore improve cost efficiency, deployment speed,

infrastructure utilisation and geographic reach. The role of local cable television and MSO and LCO ecosystems may also merit consideration in certain geographies because such networks often already possess local last-mile distribution infrastructure and neighbourhood-level presence.

C. MEASURES BY STATE GOVERNMENTS

State Governments may play a critical role through harmonised Right of Way frameworks, state fibre grid integration, simplified permissions, common duct policies, integration with transport and utility infrastructure, facilitation of power access and coordination with state digital infrastructure programmes. State-level coordination becomes especially important because fibre deployment economics are heavily influenced by Right of Way timelines, restoration costs, municipal approvals and utility coordination.

Under the Government led and supported model, State Governments can play a very important role by including deployment of PWHs under a Mission Mode program and monitor their progress after setting state wise targets to ensure that they are able to meet them. This should be taken up on priority like RoW projects.

D. MEASURES BY LOCAL BODIES AND MUNICIPALITIES

D1. Infrastructure access and simplified permissions

Local bodies and municipalities may play perhaps the most immediate operational role in enabling last-mile connectivity. Municipalities and Panchayats may facilitate access to street furniture, municipal ducts, public buildings, Smart City assets, traffic infrastructure, public power systems, local fibre corridors and local deployment planning, and simplified municipal permissions and provider-neutral infrastructure access frameworks may materially reduce deployment costs and timelines.

D2. Public Wi-Fi ready infrastructure

The concept of Public Wi-Fi ready infrastructure may also be considered in major public environments. Public buildings, transport hubs, markets, educational campuses and public institutions may progressively incorporate fibre readiness, structured cabling, mounting space, power availability and provider-neutral access capability. This may substantially reduce incremental deployment barriers.

E. COPPER INFRASTRUCTURE AS A TRANSITIONAL LAST-MILE ASSET

An additional aspect that may merit consideration is the potential use of existing copper-based last-mile infrastructure in areas where fibreisation remains incomplete. In several parts of the country, particularly in small towns, semi-urban regions, legacy commercial areas and certain institutional environments, copper local-loop infrastructure associated with

legacy landline and DSL broadband networks continues to exist. Wherever technically feasible and commercially viable, such infrastructure may continue to support moderate-capacity Public Wi-Fi deployments, especially for smaller hotspots, institutional access points, shops, Common Service Centres and community-level broadband distribution.

Also the role of LCOs and MSOs to spread the proliferation of Public WiFi must be underscored. Appropriate regulatory frameworks must be designed to facilitate this.

From the perspective of Public Wi-Fi provisioning, the key requirement is availability of reliable broadband throughput rather than exclusivity of any particular transmission medium. Accordingly, existing DSL or VDSL-based broadband connections operating over copper infrastructure may, in certain cases, support local Public Wi-Fi access where fibre deployment is not immediately available. At the same time, copper infrastructure may involve important technical limitations relating to bandwidth scalability, distance sensitivity, fault rates, maintenance complexity and suitability for high-density or high-capacity environments. Accordingly, copper-based infrastructure may be viewed primarily as a transitional and supplementary last-mile asset rather than a long-term substitute for large-scale fibreisation.

The broader long-term objective should nevertheless remain accelerated fibreisation and development of high-capacity digital infrastructure ecosystems. However, efficient utilisation of existing copper infrastructure during the transition phase may help improve speed of rollout, reduce deployment costs and accelerate initial Public Wi-Fi availability in certain underserved or partially connected geographies.

Overall, last-mile connectivity should increasingly be viewed as foundational digital infrastructure essential not only for Public Wi-Fi proliferation, but also for broader digital inclusion, digital public infrastructure access and future broadband growth.

Q13. Is there a need for the Government to provide funding for provisioning of last-mile connectivity in the uncovered or underserved areas for Public Wi-Fi networks? If yes, which funding option is best suited in the Indian context, and what should be the criteria for rural, urban, and high footfall areas, respectively? Please provide your response in detail with justification.

A. THE CASE FOR TARGETED PUBLIC SUPPORT FOR LAST-MILE CONNECTIVITY

Yes. In certain uncovered, underserved and economically difficult geographies, targeted public support for provisioning of last-mile connectivity may be justified because lack of economically viable last-mile infrastructure can prevent emergence of sustainable Public Wi-Fi ecosystems despite broader digital inclusion requirements. At the outset, however, it is important to recognise that public support should preferably focus upon enabling and catalysing ecosystem development rather than creating permanently subsidy-dependent

operational models. The support for last-mile connectivity may be more effective when directed toward enabling infrastructure rather than indefinite operational subsidisation of individual hotspots.

The preferred funding philosophy may, therefore, be targeted rather than universal, catalytic rather than permanently operational, infrastructure-oriented rather than hotspot-count-oriented and differentiated according to geography and commercial viability.

B. DIFFERENTIATED FUNDING APPROACH BY GEOGRAPHY

B1. Rural and underserved areas

Different geographies may require different funding approaches because last-mile economics differ substantially. In rural and underserved regions, last-mile connectivity may often remain commercially challenging and funding in such regions may focus primarily upon BharatNet-linked fibre extension, shared community infrastructure, institutional anchor connectivity, viability gap support, local distribution infrastructure, public infrastructure integration and common access networks. Gram Panchayat offices, schools, Common Service Centres, Primary Health Centres and post offices may function as local connectivity anchors capable of supporting broader community-level Wi-Fi ecosystems. Infrastructure grants, viability-gap mechanisms and shared-backhaul models may therefore be appropriate in such areas.

B2. Urban areas

In urban areas, however, direct funding of last-mile connectivity may generally be less necessary where commercial viability already exists. Instead, public intervention in urban environments may focus more upon municipal infrastructure enablement, common ducts, Smart City integration, street furniture access and provider-neutral deployment frameworks. Such enabling measures may materially reduce deployment costs without displacing market-led investment.

B3. Digital Bharat Nidhi as a targeted funding instrument

A specific and immediately available funding mechanism that merits explicit recommendation in this context is the Digital Bharat Nidhi. The CP notes that local bodies in rural areas can leverage DBN infrastructure for the creation or augmentation of last-mile connectivity, including in support of Public Wi-Fi deployment. BIF submits that the Authority may consider recommending that DBN eligibility criteria and disbursement frameworks be explicitly extended to support last-mile backhaul and hotspot infrastructure for Public Wi-Fi deployment, with particular focus on rural Gram Panchayats, semi-urban areas and underserved communities where market-led investment is unlikely to emerge independently in the near term.

The DBN framework, if explicitly aligned with PM-WANI deployment objectives, could function as a powerful catalyst for rural Public Wi-Fi proliferation by providing targeted capital support for the most challenging segment of the deployment chain i.e. the final kilometre from BharatNet aggregation points to actual hotspot locations. Such alignment would also improve the utilisation efficiency of DBN resources by linking disbursements to measurable connectivity outcomes rather than infrastructure creation alone. BIF accordingly urges the Authority to recommend to the Government that DBN guidelines be updated to specifically recognise Public Wi-Fi backhaul and hotspot deployment as eligible expenditure categories, with outcome linked disbursement conditions tied to operational uptime, active usage and ecosystem sustainability.

C. INFRASTRUCTURE SHARING AND EFFICIENT UTILISATION OF EXISTING PUBLIC ASSETS

Another important consideration is that funding should encourage infrastructure sharing and efficient utilisation of existing public assets. Where technically feasible and operationally appropriate, funding frameworks may support integration of municipal fibre, utility infrastructure, Smart City systems, BharatNet, transport fibre and shared digital infrastructure ecosystems.

D. ALLOCATION CRITERIA ACROSS GEOGRAPHIES

D1. Rural and underserved areas — inclusion and institutional anchors

In rural and underserved areas, criteria may include absence of broadband access, digital inclusion requirements, remoteness, institutional relevance, educational and healthcare importance and community-level impact. In this context, it is also relevant to note that India is a signatory to the United Nations Sustainable Development Goals framework, which includes commitments to affordable and inclusive digital connectivity as a foundation for broader development objectives. In view of these commitments, PM-WANI and Public Wi-Fi deployments in rural and underserved areas may be declared eligible for Corporate Social Responsibility (CSR) funding, which would attract corporate participation and supplement public resources in geographies. where market economics alone may not initially support deployment.

D2. Urban areas — fibre readiness and municipal participation

In urban environments, criteria may focus more upon fibre readiness, public-space utility, municipal participation, population density and infrastructure-sharing potential.

E. DISBURSEMENT FRAMEWORK: PERFORMANCE-LINKED AND SUSTAINABILITY-ORIENTED

Another important principle is that disbursement frameworks should progressively evolve toward performance-linked, sustainability-linked and usage-oriented approaches. Accordingly, funding may progressively consider operational uptime, actual utilisation, quality of service, continuity of operation and ecosystem sustainability rather than focusing exclusively upon initial deployment. At the same time, compliance obligations should remain proportionate so that smaller PDOs and local entrepreneurs are not discouraged from participation.

Overall, targeted support for last-mile connectivity may be justified in specific geographies and use-cases where market economics alone may not initially support ecosystem emergence. However, the long-term objective should remain sustainable infrastructure creation, local entrepreneurship, interoperable ecosystem growth and gradual transition toward commercially viable and scalable Public Wi-Fi ecosystems across India.

Q14. Are there any RoW challenges faced by service providers in accessing public places or street furniture to install Public Wi-Fi hotspots? If yes, details may be provided along with suggestions for improvements. Please provide your response in detail with justification.

A. **ROW AND MUNICIPAL INFRASTRUCTURE ACCESS AS A SIGNIFICANT DEPLOYMENT CONSTRAINT**

Yes. Right of Way and municipal infrastructure access challenges continue to constitute important operational and economic constraints affecting large-scale deployment of Public Wi-Fi ecosystems in India. It is important to recognise at the outset that scalable Public Wi-Fi proliferation, particularly in dense urban environments and high-footfall areas, depends significantly upon timely, affordable and predictable access to public infrastructure such as poles, street furniture, bus shelters, traffic infrastructure, public buildings, municipal ducts, Smart City assets and public utility infrastructure. Accordingly, access to such infrastructure should increasingly be viewed as an important component of digital infrastructure governance rather than merely a local permissions issue.

B. KEY ROW AND INFRASTRUCTURE ACCESS CHALLENGES

B1. Fragmentation and inconsistency in local approval systems

One of the principal challenges currently faced by service providers is fragmentation and inconsistency in local approval systems. Different municipalities, local bodies and public authorities often maintain different application procedures, approval timelines, fee structures, restoration conditions and infrastructure access policies. This lack of harmonisation creates deployment uncertainty, increases transaction costs, delays rollout timelines and weakens business viability, particularly for scalable hotspot ecosystems requiring deployment across multiple urban locations.

The issue becomes especially significant in the context of Public Wi-Fi because hotspot ecosystems generally require dense deployment of distributed and relatively low-footprint infrastructure. Unlike large telecom towers or major civil infrastructure projects, Public Wi-Fi equipment is typically lower-power, modular and less intrusive in nature. Therefore, approval frameworks designed for large telecom infrastructure may not always be proportionate or operationally suitable for lightweight hotspot deployments. In many cases, the process complexity itself becomes a barrier to scaling.

B2. Recurring municipal rentals and lack of transparency in access charges

Another important challenge relates to recurring municipal rentals and infrastructure access charges. Recurring rentals associated with poles, bus shelters, public buildings and street furniture may materially affect the economics of hotspot deployment, particularly in low-revenue or early-stage deployment environments. Lack of transparency and predictability in infrastructure access conditions further increases uncertainty for service providers and ecosystem participants.

C. REDEFINING THE MUNICIPAL ROLE: FROM APPROVAL AUTHORITY TO DIGITAL INFRASTRUCTURE FACILITATOR

Municipalities and local bodies may therefore play a significantly expanded role as digital infrastructure facilitators rather than merely approval-granting entities. Local authorities may facilitate access to street furniture, smart poles, municipal fibre, traffic infrastructure, public buildings and Smart City assets through transparent, standardised and non-discriminatory frameworks. This may significantly reduce deployment friction and improve scalability. In this regard, integration of Public Wi-Fi deployment with existing Smart City infrastructure may be particularly beneficial. Many cities already possess fibre-connected poles, surveillance systems, public power infrastructure and digitally enabled street infrastructure developed under Smart City and urban modernisation programmes. Public Wi-Fi deployment may often be integrated with such infrastructure at comparatively lower incremental cost, thereby improving efficiency and reducing duplication of civil works.

D. RECOMMENDED REGULATORY AND POLICY MEASURES

D1. Harmonised and simplified approval frameworks

TRAI may therefore consider recommending harmonised and simplified frameworks for Public Wi-Fi infrastructure deployment across municipalities and local bodies. Such frameworks may include standardised digital single-window systems for permissions, model municipal policies, predictable approval timelines, transparent infrastructure access charges and simplified processes for low-impact Public Wi-Fi infrastructure. The concept of deemed approvals after specified timelines may also be considered in appropriate cases to reduce procedural delays. Similarly, standardised online application systems, common

infrastructure access agreements and interoperable municipal processes may significantly improve deployment predictability and ease of doing business.

D2. Infrastructure sharing and neutral-host models

Another important consideration is infrastructure sharing. Repeated deployment of separate poles, mounting structures and power systems by multiple entities may increase costs, create visual clutter and reduce urban infrastructure efficiency. Shared and neutral-host approaches may therefore improve both deployment economics and urban infrastructure management. Such approaches may include common mounting infrastructure, shared poles, shared ducts, common power systems and municipal digital infrastructure frameworks capable of supporting multiple service providers.

D3. Public Wi-Fi ready urban infrastructure

The concept of Public Wi-Fi ready urban infrastructure may also merit consideration in future public infrastructure planning. New public infrastructure such as smart poles, transport infrastructure, pedestrian zones, public buildings and urban redevelopment projects may progressively incorporate fibre readiness, power access, mounting capability and provider-neutral digital infrastructure support. Such an approach may materially reduce future deployment friction and improve long-term scalability.

D4. Priority digital zones and coordinated municipal planning

High-footfall public environments such as transport hubs, tourism zones, public markets, educational campuses and civic centres may particularly benefit from coordinated municipal planning because such locations often require dense hotspot deployment and integrated digital service ecosystems. Local bodies may therefore support deployment planning by identifying priority digital zones, public connectivity corridors, tourism areas and major community access locations.

D5. In-building digital infrastructure and building bye-laws as a forward-looking measure

An important regulatory measure in the context of RoW and infrastructure access is the incorporation of telecom and digital infrastructure provisions into building bye-laws and construction codes. The CP notes that TRAI has previously recommended measures in this regard, and the case for such an approach has grown stronger given the CP's own acknowledgment that 70–80% of data consumption occurs indoors and that high-frequency mobile signals face inherent indoor penetration limitations.

Requiring new buildings to incorporate structured cabling, fibre access points, equipment mounting spaces, power provision and provider-neutral Wi-Fi infrastructure as part of their construction or major renovation approvals would substantially reduce the future cost and

complexity of indoor Public Wi-Fi deployment. Such a mandate need not specify the Wi-Fi operator or technology, it need only ensure that the physical infrastructure is in place so that authorised service providers can deploy hotspots without requiring civil works after occupancy. This approach, sometimes described as a digital infrastructure readiness requirement, is consistent with the Public Wi-Fi Ready framework recommended in Q1 of this submission and would make indoor Public Wi-Fi deployment a natural and low-friction activity rather than one requiring bespoke civil intervention in every building.

Overall, the preferred approach may involve harmonised municipal frameworks, simplified low-impact deployment approvals, provider-neutral infrastructure access, shared digital infrastructure models, Smart City integration and stronger municipal participation in digital infrastructure planning. Such measures may significantly reduce deployment friction, improve business viability, accelerate hotspot density and support scalable Public Wi-Fi proliferation across urban and public environments in India.

Q15. What facilitative roles can State Governments play in accelerating Public Wi-Fi deployment across rural, urban, and high-footfall areas, respectively? Should States consider deploying Public Wi-Fi networks at the municipal and gram panchayat level? Please provide your response in detail with justification.

A. THE STRATEGIC IMPORTANCE OF STATE GOVERNMENTS IN PUBLIC WI-FI PROLIFERATION

State Governments can play an extremely important enabling role in accelerating Public Wi-Fi proliferation because broadband access ecosystems are deeply influenced by state-level infrastructure conditions, municipal governance frameworks, fibreisation policies, public infrastructure access and local institutional coordination. As discussed in the responses to Questions 3, 7, 8, 12 and 14, Public Wi-Fi proliferation should evolve through a Government-enabled and market-scaled framework rather than through purely centralised operational deployment models. In this context, State Governments may function as strategic ecosystem enablers capable of integrating Public Wi-Fi proliferation with broader state-level digital infrastructure, governance and urban development initiatives.

The role of State Governments becomes particularly important because many practical aspects affecting deployment — including municipal coordination, local infrastructure access, state fibre policies, utility integration, transport infrastructure, public institutions and local approvals — fall substantially within the operational influence of state and local authorities. State Governments may therefore consider developing integrated state-level digital connectivity strategies linking fibreisation, BharatNet utilisation, Smart City programmes, municipal digital infrastructure, public-service delivery, tourism infrastructure, educational connectivity and Public Wi-Fi proliferation. Such integration may significantly improve deployment coordination and infrastructure utilisation.

B. FACILITATIVE ROLES ACROSS DIFFERENT GEOGRAPHIES

B1. Urban environments

In urban environments, State Governments may facilitate Public Wi-Fi proliferation by enabling city-level digital infrastructure ecosystems through harmonised Right of Way frameworks, common duct policies, Smart City integration, municipal fibre systems and simplified infrastructure access mechanisms. Urban Public Wi-Fi ecosystems are likely to evolve primarily through dense hotspot clusters, commercial participation, transport integration and platform-led ecosystems. Accordingly, State Governments may focus upon creating enabling conditions rather than directly operating large-scale retail hotspot systems.

B2. High-footfall areas

High-footfall urban environments such as transport hubs, markets, tourism zones, public parks and institutional districts may particularly benefit from state-supported coordination involving municipalities, transport authorities, Smart City agencies and venue owners. State-level planning and coordination may significantly improve integration of Public Wi-Fi with urban mobility systems, tourism services and digital public infrastructure ecosystems.

B3. Rural and underserved areas

In rural and underserved areas, the role of State Governments may become even more significant because commercial deployment incentives may initially remain weaker. State Governments may therefore support integration of Public Wi-Fi with BharatNet, Panchayat connectivity, educational institutions, Common Service Centre ecosystems, healthcare facilities and rural public-service delivery systems. State-level coordination may additionally improve utilisation of public assets such as government buildings, schools, Panchayat offices, public libraries, healthcare centres and utility infrastructure as anchor connectivity locations around which local Public Wi-Fi ecosystems may gradually evolve.

C. FACILITATIVE AND ENABLING ROLES

C1. Ecosystem awareness, digital literacy and local entrepreneurship

States may also facilitate ecosystem awareness, digital literacy and local entrepreneurship by coordinating with PDOAs, ISPs, trade associations, Common Service Centre networks, educational institutions and local business ecosystems. Such coordination may improve local participation and strengthen long-term sustainability.

C2. Digital infrastructure inventories and infrastructure-sharing frameworks

Another important role for State Governments may involve creation of state-level digital infrastructure inventories and infrastructure-sharing frameworks. Mapping of fibre routes, public buildings, municipal assets, utility corridors, transport infrastructure and public digital

infrastructure may materially improve deployment planning and reduce duplication of infrastructure.

D. SHOULD STATES DEPLOY PUBLIC WI-FI AT THE MUNICIPAL AND GRAM PANCHAYAT LEVEL?

D1. A balanced and differentiated approach

With regard to whether States should themselves deploy Public Wi-Fi networks at municipal and Gram Panchayat levels, a balanced and differentiated approach may be preferable. In many rural and underserved areas, direct or institution-linked deployment at Panchayat level may initially be appropriate because such locations may otherwise remain commercially unattractive during early ecosystem development stages. In such cases, Panchayat offices, schools, public institutions and BharatNet-connected facilities may function as anchor connectivity nodes capable of supporting surrounding community access.
Similarly, in certain public-interest urban environments such as public transport systems, tourism zones, educational campuses or civic spaces, state-supported or municipal-supported deployment frameworks may also be justified. However, in general, the long-term objective should preferably remain creation of sustainable and scalable ecosystems through local entrepreneurship, platform aggregation, managed-service ecosystems and market-led innovation.

D2. Preferred model: enabling and partnership-oriented frameworks

Accordingly, direct government-operated hotspot systems may be most appropriate where market failure persists, public-service objectives dominate or ecosystem catalysation is necessary. In commercially viable environments, enabling and partnership-oriented frameworks may generally produce more sustainable outcomes than fully state-operated retail hotspot systems. PPP models, managed-service arrangements and provider-neutral deployment frameworks may therefore be preferable in many environments because they preserve innovation, operational flexibility, commercial sustainability and ecosystem scalability.

Overall, State Governments may play a transformational role in Public Wi-Fi proliferation by functioning as digital infrastructure enablers, ecosystem coordinators, fibreisation facilitators, public asset integrators and inclusion accelerators, while allowing scalable service ecosystems to evolve through interoperable and market-led participation frameworks.

Q16. Should the State Government need to take initiatives to improve the availability of last-mile connectivity for Public Wi-Fi networks? If yes, what measures can incentivise States /municipalities to undertake city- and town-level fiberisation to ensure Public Wi-Fi network proliferation? Please provide your response in detail with justification.

A. THE CRITICAL ROLE OF STATE GOVERNMENTS IN LAST-MILE FIBREISATION

Yes. State Governments may play a highly important role in improving availability of last-mile connectivity because the proliferation of Public Wi-Fi ecosystems is fundamentally dependent upon dense, reliable and economically viable local broadband infrastructure. As discussed in the response to Question 12, the challenge in many parts of India is not merely availability of middle-mile connectivity, but economically viable local last-mile distribution capable of supporting scalable hotspot ecosystems. State Governments and municipalities are particularly important in this context because city and town level fibreisation depends substantially upon local Right of Way conditions, municipal coordination, public infrastructure access, utility integration, transport infrastructure and local deployment economics.

Accordingly, State Governments may significantly accelerate Public Wi-Fi proliferation by treating fibreisation as foundational digital infrastructure similar to roads, electricity or urban utility systems.

B. KEY MEASURES STATE GOVERNMENTS MAY ADOPT

B1. Harmonised and simplified RoW frameworks

One of the most important measures may be development of harmonised and simplified Right of Way frameworks across cities and towns. Delays, fragmented permissions and inconsistent municipal practices significantly increase deployment costs and reduce viability of local fibre expansion. States may therefore establish harmonised state-level Right of Way frameworks, common approval processes, standard restoration norms, digital application systems and time-bound approval mechanisms.

B2. Common duct and utility corridor policies

Another important measure may involve promotion of common duct and utility corridor policies. Integration of fibre deployment with road construction, urban redevelopment, Smart City projects and utility infrastructure may substantially reduce future fibre deployment costs and avoid repeated excavation. State Governments may additionally encourage municipalities to progressively develop municipal fibre systems, provider-neutral duct infrastructure, shared digital infrastructure corridors and public digital utility frameworks. Such approaches may improve infrastructure efficiency and reduce duplication.

B3. Integration with Smart City and urban digital infrastructure programmes

An important opportunity may also lie in integration of Public Wi-Fi proliferation with broader Smart City and urban digital infrastructure programmes. Many cities already possess fibre-connected surveillance systems, smart poles, command-and-control infrastructure and

municipal digital assets. Public Wi-Fi and last-mile broadband expansion may often be integrated with such infrastructure at comparatively lower incremental cost.

B4. Utilisation of public infrastructure and shared deployment frameworks

State Governments may also facilitate utilisation of public infrastructure such as transport systems, public buildings, electricity infrastructure, utility corridors and institutional campuses for extending local fibre and broadband access networks. Another important consideration is that State policies encouraging shared ducts, common fibre corridors, municipal infrastructure sharing and provider-neutral access frameworks may materially improve deployment economics and accelerate proliferation.

C. INCENTIVISING MUNICIPALITIES TO UNDERTAKE CITY- AND TOWN-LEVEL FIBREISATION

C1. Linking fibreisation with urban development programmes and outcomes

Incentivising municipalities to undertake fibreisation may require both policy support and economic alignment. State Governments may therefore consider linking urban digital infrastructure programmes and Smart City initiatives with measurable fibreisation and digital-connectivity outcomes. Municipalities undertaking proactive fibreisation and digital infrastructure planning may be supported through state digital infrastructure programmes, Smart City integration, infrastructure grants, technical assistance, planning support and digital governance incentives.

C2. Capacity-building and technical guidance

Capacity-building support may also be important because many municipalities may not presently possess sufficient technical expertise relating to fibre planning, neutral-host infrastructure models or digital urban infrastructure management. State-level guidance frameworks, model municipal policies and technical support systems may therefore improve implementation quality.

C3. Smaller towns, semi-urban areas and rural Panchayats

In smaller towns and semi-urban areas, fibreisation economics may remain relatively weaker. In such locations, States may facilitate aggregated infrastructure planning, shared backbone models, BharatNet integration and coordinated deployment across public institutions and commercial zones. The role of Panchayats may also be important in rural environments where BharatNet-connected locations may serve as local aggregation points for surrounding Wi-Fi ecosystems.

D. FIBREISATION AS FOUNDATIONAL DIGITAL PUBLIC INFRASTRUCTURE

Another important aspect is that fibreisation should be viewed not only as telecom infrastructure creation, but as foundational digital public infrastructure supporting broadband access, e-governance, digital payments, education, telemedicine, tourism, transport systems and broader digital economy growth. Accordingly, incentives for city- and town-level fibreisation may be framed not merely as telecom-sector initiatives, but as broader economic and digital development priorities.

Overall, State Governments and municipalities may significantly accelerate Public Wi-Fi proliferation by simplifying local fibre deployment, integrating fibreisation with urban planning, enabling shared infrastructure, leveraging public assets, harmonising Right of Way frameworks and treating local broadband infrastructure as essential digital infrastructure for future economic growth and digital inclusion.

Q.17. What facilitative roles can local bodies play in accelerating the deployment and sustainable operation of Public Wi-Fi networks in rural and urban areas? Please provide your response in detail with justification.

A. LOCAL BODIES AS CRITICAL ENABLERS OF PUBLIC WI-FI DEPLOYMENT

Local bodies may play one of the most critical operational and enabling roles in accelerating deployment and sustainable operation of Public Wi-Fi ecosystems because Public Wi-Fi is inherently location-specific and highly dependent upon local infrastructure, public-space access, municipal coordination and community-level participation. As discussed in the responses to Questions 3, 9, 12 and 14, scalable Public Wi-Fi proliferation ultimately depends not only upon national policy frameworks, but also upon local execution ecosystems capable of supporting dense deployment, infrastructure access, public-space integration, fibre readiness and long-term operational sustainability. Accordingly, municipalities, urban local bodies and Panchayats may increasingly function as local digital infrastructure facilitators rather than merely approval-granting authorities.

B. ROLE OF URBAN LOCAL BODIES

B1. Infrastructure access and simplified deployment frameworks

In urban environments, local bodies may play an especially important role in enabling access to street furniture, poles, smart poles, bus shelters, traffic infrastructure, municipal fibre, public buildings, parks, transport systems and Smart City infrastructure. Such infrastructure may significantly reduce deployment costs and improve scalability of hotspot ecosystems. Municipalities may additionally facilitate simplified permissions, harmonised local processes, transparent infrastructure access frameworks, digital single-window systems and provider-neutral deployment environments. These measures may materially improve ease of deployment and reduce operational uncertainty for ecosystem participants.

B2. Spatial planning and Smart City integration

Another important role for urban local bodies may involve spatial planning of Public Wi-Fi ecosystems. Rather than isolated hotspots, municipalities may help identify hotspot clusters, digital corridors, tourism zones, transport hubs, public markets, educational districts and high-footfall public environments where deployment may create greater user value and ecosystem sustainability. Municipalities may also integrate Public Wi-Fi planning with Smart City initiatives, public transport systems, tourism infrastructure, urban redevelopment projects and digital public-service delivery platforms.

C. ROLE OF PANCHAYATS AND RURAL LOCAL BODIES

In rural environments, Panchayats and local rural bodies may play an equally important facilitative role, though the operational context differs. Rural Public Wi-Fi ecosystems may initially depend more heavily upon shared access, community-level usage, institutional anchors and public-service integration. Accordingly, Panchayats may support deployment through identification of public access locations, integration with BharatNet-connected facilities, community awareness initiatives, support for local entrepreneurship and coordination with schools, Common Service Centres, healthcare centres and public institutions. Panchayat buildings, schools, libraries, public service centres and community institutions may additionally function as anchor connectivity locations around which local Wi-Fi ecosystems may evolve.

D. FACILITATIVE ROLES OF LOCAL BODIES

D1. Local demand aggregation

Another important role for local bodies may involve local demand aggregation. In many locations, individual hotspots may not independently become commercially viable. However, coordinated local demand across markets, institutions, public offices, tourism areas, transport points and community facilities may improve deployment viability and encourage participation by ISPs, PDOAs and platform providers.

D2. Digital literacy and ecosystem awareness

Local bodies may also support digital literacy and ecosystem awareness. Public Wi-Fi adoption ultimately depends not merely upon hotspot deployment, but upon user familiarity, trust and habitual usage. Accordingly, local awareness campaigns, digital literacy initiatives and integration with local public services may materially improve uptake.

E. PREFERRED MODEL: LOCAL BODIES AS ENABLERS RATHER THAN OPERATORS

At the same time, local bodies should function as enabling and coordinating entities rather than excessively interventionist operational entities in commercially viable markets. Long-term ecosystem sustainability is likely to emerge more effectively through managed-service ecosystems, local entrepreneurship, interoperable platform participation and commercially sustainable deployment models. Accordingly, PPP models, provider-neutral infrastructure frameworks and partnership-oriented deployment approaches may generally produce more sustainable outcomes than fully government-operated hotspot systems in commercially viable areas. Local bodies may therefore focus primarily upon reducing deployment friction, enabling infrastructure access, integrating public assets, facilitating local coordination and supporting inclusive digital infrastructure planning.

Overall, municipalities and Panchayats may play a transformational role in Public Wi-Fi proliferation by functioning as local digital infrastructure facilitators, ecosystem coordinators, public asset enablers and community-level digital inclusion partners. Such an approach may significantly accelerate both deployment and long-term sustainability of Public Wi-Fi ecosystems across diverse Indian geographies.

Q18. What regulatory or policy incentives, schemes or programs are required to promote active participation of TSPs and ISPs in Public Wi-Fi deployment? Please provide your response in detail with justification.

A. THE STRATEGIC IMPORTANCE OF TSP AND ISP PARTICIPATION

The long-term scalability and sustainability of Public Wi-Fi ecosystems in India will depend substantially upon the meaningful participation of Telecom Service Providers and Internet Service Providers. At present, Public Wi-Fi is often perceived as a peripheral or standalone connectivity layer rather than as an integrated component of India's broader broadband growth architecture. However, as discussed in the responses to Questions 1, 2, 4, 7 and 9, Public Wi-Fi has the potential to evolve into a complementary broadband access layer capable of supporting traffic densification, indoor capacity augmentation, broadband inclusion, high-capacity usage and broader digital ecosystem expansion.

Accordingly, the objective of policy and regulatory frameworks should not be to impose rigid operational obligations upon TSPs and ISPs, but rather to create an enabling environment where participation in Public Wi-Fi deployment becomes both commercially attractive and strategically beneficial. A collaborative and incentive-driven framework is likely to produce more sustainable outcomes than a compliance-oriented approach.

B. PUBLIC WI-FI AS A COMPLEMENTARY LAYER TO MOBILE BROADBAND

It is important to recognise that India's mobile broadband success has been globally significant and has enabled large-scale digital inclusion. At the same time, the CP highlights the widening gap between India and several advanced digital economies in terms of fixed

broadband penetration, fibre deployment and the proportion of traffic carried over fixed networks. As broadband consumption increasingly shifts toward high-capacity applications such as HD video streaming, cloud computing, AI-enabled services, enterprise connectivity, digital education and immersive technologies, the importance of a complementary fixed broadband and Wi-Fi ecosystem will continue to grow. In this context, Public Wi-Fi should be viewed not as a substitute for mobile broadband, but as a complementary and capacity-enhancing layer within India's overall broadband ecosystem.

Particularly in indoor environments, high-footfall locations and dense urban areas, interoperable Wi-Fi ecosystems can improve user experience, reduce congestion on mobile networks and support more efficient broadband delivery.

B. KEY REGULATORY AND POLICY INCENTIVES REQUIRED

C1. Commercially viable traffic offload and integrated broadband participation models

One of the most significant opportunities lies in the gradual development of commercially viable traffic offload and integrated broadband participation models. As mobile data consumption continues to rise, especially in urban and indoor environments, managed Wi-Fi ecosystems can contribute to improved network efficiency and enhanced customer experience. Regulatory frameworks that encourage voluntary and commercially negotiated offload arrangements between TSPs, ISPs, PDOAs and managed hotspot operators may therefore help align Public Wi-Fi proliferation with broader broadband ecosystem objectives.

C2. Broadband market expansion through Public Wi-Fi enablement

ISPs should increasingly be encouraged to view Public Wi-Fi enablement not merely as an additional operational responsibility, but as an opportunity for broadband market expansion. Wider exposure of users to high-capacity broadband environments may stimulate greater adoption of fixed broadband services and higher-capacity plans. In this manner, Public Wi-Fi can contribute not only to hotspot usage but also to long-term broadband demand creation.

C3. Simplified onboarding and technical integration frameworks for smaller ISPs

At the same time, the present ecosystem continues to face practical constraints that limit ISP participation. Many smaller ISPs have not yet meaningfully integrated with the PM-WANI ecosystem due to uncertainty regarding long-term commercial viability, limited operational familiarity with PM-WANI onboarding processes, lack of standardised technical integration frameworks, absence of scalable onboarding support systems and uncertainty regarding customer demand. In this regard, standardised onboarding support, simplified technical integration frameworks and interoperable operational toolkits may significantly improve participation by smaller ISPs and regional broadband providers.

C4. PM-WANI-ready CPE and voluntary hotspot activation frameworks

Another important consideration relates to customer premises equipment and hotspot enablement capability. Over time, there may be merit in encouraging the development of PM-WANI-ready broadband ecosystems wherever technically feasible and commercially appropriate. Standardised secondary SSID capability and interoperable firmware architectures may gradually improve the ease of hotspot enablement, particularly for commercial establishments and community-facing broadband environments. Over time, broadband subscribers and establishments willing to participate in Public Wi-Fi ecosystems may be enabled to activate managed hotspot functionality through simplified digital onboarding journeys integrated with ISP or platform applications, which may substantially simplify participation by small establishments and local entrepreneurs while preserving customer consent, operational flexibility and commercial innovation across the ecosystem.

However, any such evolution should remain technology-neutral, operationally practical, privacy-sensitive, commercially sustainable and based upon informed consumer participation. The consultation process may therefore consider whether simplified and voluntary activation frameworks can reduce operational friction for potential PDO participation. For example, where broadband subscribers voluntarily choose to participate in PM-WANI ecosystems, onboarding and activation mechanisms may become simpler through integration with ISP applications, digital KYC systems and interoperable backend architectures.

C5. Commercially sustainable bandwidth provisioning frameworks

Another critical factor affecting ecosystem participation is the affordability and commercial viability of bandwidth provisioning for Public Wi-Fi environments. Sustainable proliferation will require economically viable FTTH and broadband provisioning frameworks capable of supporting hotspot operations, particularly for smaller PDOs and local entrepreneurs. In this context, pricing structures for Public Wi-Fi-linked broadband provisioning will play a crucial role in determining ecosystem scalability. The long-term objective should therefore be to ensure that bandwidth provisioning frameworks remain commercially sustainable while simultaneously enabling economically viable hotspot operations and broad-based ecosystem participation. Predictable and scalable commercial structures can improve participation by ISPs, PDOAs and local entrepreneurs alike.

C6. Interoperable and standardised operational frameworks

TRAI may therefore consider encouraging interoperable and standardised hotspot products, simplified onboarding systems, managed-service participation frameworks, infrastructure sharing, municipal infrastructure access and commercially sustainable broadband provisioning architectures. Such measures can reduce operational complexity and improve ecosystem scalability.

C7. Enabling 5G–Wi-Fi convergence and heterogeneous network participation

The CP identifies seamless 5G–Wi-Fi integration as a defining characteristic of the emerging digital connectivity landscape, and international deployments are already demonstrating that 5G and Wi-Fi will increasingly function as complementary and interoperable layers within a unified broadband delivery architecture rather than as competing standalone technologies.

For TSPs deploying 5G networks in India, Wi-Fi, and specifically Public Wi-Fi supported by PM-WANI, represents a natural and cost-efficient indoor coverage and traffic offload complement. High-frequency 5G signals, while offering high throughput, face inherent indoor penetration limitations. Wi-Fi 6 and Wi-Fi 7 systems, anchored on fixed broadband backhaul and operating in the 5 GHz and 6 GHz bands, can provide the dense indoor coverage and high-capacity shared access that 5G alone cannot economically deliver in every environment.

D. THE ROLE OF PDOAS, APP PROVIDERS AND SCALABLE PLATFORM ECOSYSTEMS

The role of App Providers and PDOAs will also become increasingly important because scalable platform entities can aggregate demand, simplify onboarding, improve customer discovery, support roaming, manage billing and create commercially scalable participation models. As discussed in the response to Question 4, scalable aggregation layers may help transform fragmented hotspot deployments into interoperable digital ecosystems capable of generating broader user familiarity and repeat usage. Serious ecosystem players can create investment-grade models and TSPs and ISPs may find commercially scalable opportunities. TSPs and ISPs may partner with large interoperable platform ecosystems, scalable managed service architectures can reduce operational fragmentation and platform-led Wi-Fi ecosystems can create meaningful broadband augmentation opportunities.

Overall, the preferred policy approach should focus on creating an ecosystem where TSPs and ISPs increasingly view Public Wi-Fi not as a competing or isolated connectivity layer, but as a complementary broadband growth opportunity capable of enhancing customer experience, supporting network efficiency, improving broadband adoption, strengthening fixed broadband ecosystems and expanding India's long-term digital infrastructure capacity. Such an approach would create stronger alignment between national broadband objectives, commercial sustainability, digital inclusion and long-term ecosystem scalability.

Q19. What regulatory or fiscal incentives, schemes or programs may be required in the provisioning of bandwidth and backhaul for Public Wi-Fi networks? Please provide your response in detail with justification.

A. AFFORDABLE BANDWIDTH AND BACKHAUL AS FOUNDATIONAL REQUIREMENTS FOR SUSTAINABLE PUBLIC WI-FI

Provisioning of affordable, reliable and scalable bandwidth and backhaul remains one of the most important foundational requirements for sustainable Public Wi-Fi proliferation in India. As discussed in the responses to Questions 12 and 13, the long-term viability of hotspot ecosystems depends fundamentally upon the strength of underlying broadband infrastructure and economically viable last-mile connectivity. In this context, the availability of robust and affordable backhaul infrastructure is central to the success of Public Wi-Fi ecosystems.

It is important to recognise at the outset that Public Wi-Fi ecosystems can scale sustainably only when bandwidth provisioning frameworks remain commercially workable for PDOAs, local entrepreneurs, institutions, venue operators, ISPs and TSPs. Accordingly, the objective of regulatory and policy frameworks should be to reduce infrastructure friction, improve broadband accessibility and strengthen ecosystem viability rather than create permanently subsidy-dependent operational models. A commercially sustainable ecosystem, rather than one dependent upon continuous subsidies, is likely to produce stronger long-term outcomes for broadband expansion and digital inclusion.

B. INFRASTRUCTURE-ORIENTED REGULATORY AND FISCAL INCENTIVES

B1. Accelerated fibreisation and open-access digital infrastructure

One of the most important requirements may be accelerated fibreisation and the development of open-access digital infrastructure. Public Wi-Fi proliferation is closely linked with the availability of economically viable backhaul capable of supporting high-capacity usage, dense hotspot deployment, roaming ecosystems and scalable user adoption. Measures encouraging fibre expansion, common ducts, shared digital infrastructure, neutral-host backhaul systems, municipal fibre access, utility corridor integration and provider-neutral infrastructure access may significantly improve deployment economics and reduce barriers to expansion.

B2. Utilisation of existing infrastructure assets

An equally important opportunity may lie in the more efficient utilisation of existing infrastructure assets associated with BharatNet, RailTel, PowerGrid, Smart City infrastructure, municipal fibre systems, utility networks and cable or MSO ecosystems, wherever technically feasible and operationally appropriate. Shared infrastructure approaches may materially reduce duplication of costs, improve geographic reach and accelerate deployment timelines.

B3. BharatNet integration and rural broadband deepening

The long-term success of rural Public Wi-Fi proliferation may depend significantly upon deeper operational integration between BharatNet and PM-WANI ecosystems. BharatNet may progressively evolve not merely as a fibre deployment initiative, but as an active and open-access rural broadband distribution backbone capable of supporting scalable last-mile Public Wi-Fi ecosystems. In this regard, transparent wholesale access frameworks, defined service-level standards, uptime accountability and simplified access arrangements for licensed ISPs may materially improve utilisation of BharatNet infrastructure. Simultaneously, India may benefit from gradual extension of regional peering and edge caching ecosystems closer to BharatNet aggregation points and district or block-level nodes. Such localisation of traffic may significantly reduce rural bandwidth costs, improve latency, reduce upstream transit dependence and strengthen long-term viability of rural Public Wi-Fi deployments.

B4. Infrastructure sharing and provider-neutral access frameworks

Another important requirement may be the promotion of infrastructure sharing and provider-neutral access frameworks. Repeated duplication of fibre and backhaul infrastructure may increase deployment costs and reduce viability, particularly in low-density and emerging markets. Shared fibre systems, common ducts, neutral-host infrastructure and municipal digital infrastructure frameworks may therefore significantly improve cost efficiency and support broader ecosystem scalability.

C. COMMERCIALLY VIABLE BROADBAND PROVISIONING FRAMEWORKS

C1. Economically viable bandwidth pricing for Public Wi-Fi environments

Another important consideration relates to economically viable broadband provisioning for Public Wi-Fi environments. Sustainable hotspot ecosystems require bandwidth pricing structures capable of supporting viable retail and community-level operations, particularly for smaller PDOs and local entrepreneurs operating in low-margin environments. In this context, predictable and scalable commercial provisioning frameworks may significantly improve ecosystem participation and long-term sustainability. The objective may therefore be to ensure that Public Wi-Fi-linked broadband provisioning remains commercially workable while continuing to preserve incentives for infrastructure investment and network expansion.

C2. Standardised managed hotspot bandwidth products

The consultation process may also consider whether standardised managed hotspot bandwidth products could improve operational simplicity and encourage wider ISP participation. Standardised hotspot broadband plans, managed Wi-Fi service bundles, scalable enterprise hotspot solutions and integrated PM-WANI participation frameworks may simplify deployment and operational management. Such simplified operational architectures may particularly help smaller ISPs and regional broadband providers participate more actively in the ecosystem.

D. TARGETED SUPPORT FRAMEWORKS AND SECTORAL DEPLOYMENT MODELS

D1. Rural and underserved areas

In rural and underserved areas, targeted support for backhaul and local distribution infrastructure may also be justified where commercial viability remains weak. As discussed in the response to Question 13, such support may focus upon enabling infrastructure and ecosystem catalysation rather than indefinite operational subsidisation. BharatNet-connected institutions, Panchayat infrastructure and public-service facilities may function as local aggregation points capable of supporting surrounding Wi-Fi ecosystems. Integration of Public Wi-Fi with educational institutions, healthcare centres, Common Service Centres and public-service infrastructure may improve utilisation, affordability and long-term sustainability.

D2. High-footfall environments

High-footfall environments such as transport systems, tourism zones, educational campuses and public institutions may additionally benefit from PPP-oriented backhaul frameworks, shared infrastructure models and venue-level broadband integration. Such approaches may improve deployment viability while ensuring that connectivity infrastructure is utilised efficiently across multiple stakeholders and user groups.

E. OPERATIONAL INTEGRATION AND THE ROLE OF STATE GOVERNMENTS AND MUNICIPALITIES

E1. Simplified operational integration between ISPs, PDOAs and App Providers

Another important area may involve simplifying operational integration between ISPs, PDOAs and App Providers. Standardised APIs, interoperable backend systems and simplified onboarding frameworks may reduce operational complexity, improve interoperability and encourage wider participation across the ecosystem.

E2. State Government and municipal facilitation of backhaul infrastructure

The role of State Governments and municipalities may also be important in improving backhaul availability through harmonised Right of Way frameworks, municipal fibre systems, Smart City integration, utility corridor access and public infrastructure facilitation. Such measures may materially reduce deployment friction, improve fibre reach and accelerate broadband expansion into underserved areas.

Overall, the preferred approach may involve accelerated fibreisation, shared digital infrastructure, open-access backhaul ecosystems, economically viable provisioning frameworks, simplified ISP participation and infrastructure-oriented ecosystem support.

Such an approach may improve both affordability and scalability of Public Wi-Fi ecosystems while preserving long-term incentives for broadband investment, innovation and sustainable digital infrastructure growth. A balanced framework combining infrastructure enablement, commercial sustainability and collaborative ecosystem participation may provide the strongest foundation for long-term Public Wi-Fi expansion in India.

Q20. What measures can be adopted to incentivise private enterprises, commercial establishments, shop owners, community institutions, etc., to install Public Wi-Fi hotspots? Please provide your response in detail with justification.

A. THE ROLE OF PRIVATE ESTABLISHMENTS AND COMMUNITY INSTITUTIONS IN PUBLIC WI-FI PROLIFERATION

Private enterprises, commercial establishments, shop owners, community institutions and public-facing premises are one of the most important drivers of Public Wi-Fi proliferation in India. Unlike purely infrastructure-led deployment models, **participation by such entities can create a demand-driven and locally distributed Public Wi-Fi ecosystem.** This is particularly important because shops, cafes, clinics, educational institutions, community centres, transport-linked establishments and small businesses are often **located exactly where users require affordable and convenient connectivity.**

At the outset, it is important to recognise that the question is not limited to PM-WANI alone, but to the broader proliferation of Public Wi-Fi. However, **PM-WANI remains a very important enabling framework because it has already created a light-touch architecture under which local establishments can participate in broadband access provisioning without becoming telecom licensees. The task now is to create confidence, visibility and commercial incentives so that this enabling framework results in actual deployment.**

B. FOUNDATIONAL INCENTIVES FOR PRIVATE AND COMMUNITY PARTICIPATION

B1. Regulatory certainty and policy confidence

A critical requirement is regulatory certainty and policy confidence. Many potential participants may hesitate to invest in hotspot devices, broadband upgrades or customer-facing Wi-Fi services if they are unsure whether the policy framework will remain stable, whether the model will scale, or whether future regulatory changes may alter the economics. It should, therefore, **be clearly communicated that Public Wi-Fi and PMWANI based Public WiFi which is Government's own indigenously created decentralized Public WiFi based on a ' light touch ' framework is a continuing and important component of India's broadband strategy and that frameworks such as PM-WANI are intended to evolve and mature rather than be reversed. This assurance is important for**

encouraging investment by PDOAs, App Providers, ISPs, entrepreneurs and commercial establishments.

B2. Awareness and market education

Another important requirement is awareness and market education. **Many shop owners and small enterprises may not be aware that they can participate in Public Wi-Fi deployment or that the regulatory framework has been substantially liberalised.** Even where awareness exists, they may perceive Public Wi-Fi as technically complex, risky or commercially uncertain. This perception can be addressed through structured awareness initiatives led by ISPs, PDOAs, App Providers, local trade associations, municipalities, Common Service Centre networks and community institutions. **The message should be simple: a shopkeeper or establishment should be able to view Public Wi-Fi enablement as a digital business service, similar in simplicity to accepting UPI payments or joining an online commerce platform.**

B3. Easy procurement, activation and managed operation

The most important operational incentive would be to make Public Wi-Fi **deployment easy to procure, easy to activate and easy to operate**. Commercial establishments located in broadband-served areas should be able to obtain managed Public Wi-Fi connectivity from authorised providers through **standardised retail or business offerings**. Such offerings may include the broadband connection, hotspot device, authentication system, captive portal, security configuration, backend support, remote monitoring and customer support. The establishment should not be required to manage telecom-grade technical complexity.

This approach would create a **practical right to procure Public Wi-Fi connectivity for commercial and community-facing establishments** wherever fixed broadband infrastructure exists and provisioning is technically feasible. This would convert Public Wi-Fi from an abstract policy possibility into an actual procurable service category.

B4. Low entry cost and managed-service deployment models

A further incentive is low entry cost deployment. Many small establishments may not wish to make upfront investments in routers, access points, maintenance systems or software integration. **Managed-service models, device leasing, revenue-sharing hotspot kits and broadband-plus-public-Wi-Fi bundles can reduce participation barriers.** The local establishment may then participate without significant capital expenditure, while the ISP, PDOA or platform provider manages the technical layer.

C. COMMERCIAL INCENTIVES AND VALUE-ADDED MODELS

C1. Local digital commerce and customer engagement benefits

Commercial establishments also require a clear business reason to participate. The incentive should not be framed only as resale of data. **Public Wi-Fi can create multiple indirect benefits for shops and institutions. It can increase customer footfall, improve dwell time, enable digital engagement, support local advertising, improve customer loyalty, provide digital coupons, enable local offers and strengthen the establishment's visibility in the neighbourhood. App Providers and PDOAs can play an important role in creating such value-added models.**

For example, a shop offering Public Wi-Fi may also be discoverable on a Public Wi-Fi application, may display offers through the captive portal, may provide purchase-linked access, or may participate in local digital promotion campaigns. In this manner, Public Wi-Fi can become a local digital commerce and customer engagement layer, not merely a connectivity resale activity.

C2. Simplified voluntary onboarding for broadband subscribers

At the same time, broadband subscribers, I.e. shops, cafes and other commercial entities, who voluntarily wish to participate as PDOs may be supported through simplified digital onboarding. Over time, ISPs may integrate Public Wi-Fi activation features into subscriber applications so that eligible users or establishments can opt in easily. However, such participation should remain consent-based, secure and operationally manageable.

C3. Platform-led aggregation through PDOAs and App Providers

Another important measure is platform-led aggregation. **Individual shops may not have the ability to attract users, manage billing, create roaming packs or run promotional campaigns. Scaled PDOAs and App Providers can aggregate thousands of such establishments into recognisable and trusted Public Wi-Fi networks.** This can create confidence for both users and shopkeepers. It can also enable roaming, common branding, application-based discovery, digital payments, customer support and settlement systems. **Incentives for private participation should therefore include not only support for the individual hotspot, but also support for the broader ecosystem of PDOAs and App Providers. If these platform layers become mature and innovative, they can make Public Wi-Fi participation more attractive for small establishments.**

D. INCENTIVES FOR COMMUNITY INSTITUTIONS AND INCLUSION-ORIENTED PARTICIPATION

Community institutions such as schools, libraries, Resident Welfare Associations, community centres, NGOs, Panchayat facilities, religious institutions and public-service centres may have a different incentive structure. For them, **the value may lie in enabling education, e-governance, telemedicine, digital payments, online applications, community information and digital inclusion. Such institutions may be supported**

through managed connectivity models, institutional partnerships and targeted public interest deployment support.

E. LOCAL COORDINATION, MUNICIPAL SUPPORT AND CLUSTER DEPLOYMENT MODELS

Municipalities and local bodies can also support private participation by identifying high-potential areas such as markets, transport nodes, public parks, tourism zones, educational clusters and commercial streets. When local bodies facilitate infrastructure access, awareness, local permissions and market-level coordination, private establishments are more likely to participate.

In **high-footfall commercial areas, Public Wi-Fi deployment may be encouraged through local cluster models rather than isolated individual hotspots.** For example, a market association or commercial street may coordinate with an ISP, PDOA or App Provider to create a Public Wi-Fi zone. This improves user experience, increases visibility and improves the commercial case for participating establishments.

F. TRUST, SECURITY ASSURANCE AND COMMERCIAL FLEXIBILITY

F1. Security and liability assurance for participating establishments

Another important measure is trust and security assurance. Shop owners and institutions may hesitate to provide Public Wi-Fi if they fear misuse, liability or security complications. Therefore, managed Public Wi-Fi services should include clear user authentication, lawful traceability, user isolation, traffic separation from the establishment's private network and backend compliance support. This will reduce perceived risk and improve participation. For details on Public Trust and Safety, BIF has made some clear Recommendations which are enclosed in Annexure-I. We urge the Authority to kindly recommend the same to the Government for implementation.

F2. Commercially flexible participation models

Finally, the incentive framework should be **commercially flexible.** Different establishments will participate for different reasons. Some may seek direct revenue share. Some may seek customer engagement. Some may want to provide free access as a service. Some may integrate Wi-Fi with purchases. Some community institutions may use it for social inclusion. **The framework should therefore not assume a single business model.**

Incentivising private enterprises, commercial establishments, shop owners and community institutions requires a combination of regulatory certainty, awareness, ease of onboarding, low entry cost, managed-service support, platform aggregation, local digital commerce integration and trust-building. The objective should be to make Public Wi-Fi deployment

simple, safe, trustworthy and commercially meaningful for local establishments. If this is achieved, private and community participation can become a powerful driver of Public Wi-Fi density and geographic spread, enabling India to build a distributed, affordable and high-capacity broadband access layer.

Q21. Is there a need to strengthen the role of public or private entities as system integrators for the deployment of Public Wi-Fi networks? If yes, what policy or institutional support may be required? Please provide your response in detail with justification.

A. THE CRITICAL NEED FOR STRONG SYSTEM INTEGRATION IN PUBLIC WI-FI ECOSYSTEMS

Yes. Strengthening the role of capable public and private system integrators is likely to become one of the most important requirements for achieving scalable, interoperable and commercially sustainable Public Wi-Fi proliferation in India. It is important to recognise at the outset that large-scale Public Wi-Fi ecosystems cannot evolve sustainably through fragmented and isolated hotspot deployments alone. While the PM-WANI framework has appropriately adopted a light-touch and decentralised participation model for PDOs, **the long-term scalability of the ecosystem will depend substantially upon the existence of strong aggregation, orchestration and managed-service layers capable of integrating thousands of distributed hotspots into trusted and usable digital connectivity ecosystems.**

In practical terms, most small PDOs, shop owners, institutions and local establishments are unlikely to possess the technical, operational or commercial capability to independently manage critical functions such as authentication systems, roaming integration, cybersecurity, backend monitoring, billing systems, analytics, settlement systems, customer support, software upgrades, interoperability and network operations. As a result, scalable Public Wi-Fi ecosystems may require the **emergence of specialised entities capable of functioning as system integrators, managed-service providers, aggregation platforms and operational coordinators.**

Such entities may include PDOAs, App Providers, ISPs, managed-service operators, neutral-host providers, enterprise connectivity providers, municipal digital infrastructure entities and specialised Wi-Fi platform companies. Their role may extend far beyond simple technical integration. In reality, **these entities may become the operational backbone of scalable Public Wi-Fi ecosystems.**

B. HOW SYSTEM INTEGRATORS ADDRESS CURRENT ECOSYSTEM LIMITATIONS

As discussed in earlier responses, one of the principal challenges currently affecting Public Wi-Fi proliferation is that the ecosystem remains highly fragmented and operationally

immature. Individual hotspots often remain isolated, difficult to discover and commercially unsustainable. Users frequently experience fragmented onboarding systems, repeated authentication requirements and inconsistent quality of service, while local establishments often lack operational support and confidence in managing such systems.

System integrators can address many of these limitations by creating **aggregated and interoperable ecosystems capable of delivering seamless onboarding, roaming continuity, standardised user experiences, unified customer interfaces, backend settlement systems, digital payments, analytics, remote monitoring, fraud management, customer support and platform-level innovation**. I**n this sense, system integrators may play a role similar to digital aggregation platforms in other sectors of the digital economy.**

This issue becomes particularly important because **Public Wi-Fi proliferation is not merely an infrastructure challenge, it is equally a usability, trust and ecosystem-management challenge**. Strong system integration frameworks may therefore significantly improve user confidence, hotspot discoverability, roaming capability, operational reliability, commercial viability and investor confidence.

C. SYSTEM INTEGRATORS AS CATALYSTS FOR INVESTMENT AND SCALE

C1. Attracting long-term investment into the Public Wi-Fi ecosystem

Another important aspect is that **scalable system integrators may help attract serious long-term investment into the Public Wi-Fi ecosystem.** At present, many investors, ISPs and platform players may perceive Public Wi-Fi deployments as fragmented, operationally uncertain and commercially immature. However, **if robust aggregation and managed-service ecosystems emerge, Public Wi-Fi may increasingly evolve into a scalable digital infrastructure and platform opportunity rather than merely a collection of isolated hotspots.**

C2. Importance in high-footfall, enterprise and rural environments

The role of **system integrators may become particularly important in high-footfall environments, enterprise ecosystems, Smart City deployments, transport systems, tourism zones and institutional networks** where interoperability, roaming, analytics, high-capacity management, security and operational continuity become critical requirements. Similarly, **in rural and community environments, managed system integrators may help local institutions and small entrepreneurs participate effectively without requiring telecom-grade technical expertise.**

D. COMPATIBILITY WITH PM-WANI'S DECENTRALISED AND LIGHT-TOUCH PHILOSOPHY

Another important consideration is that strengthening system integrator participation does not require moving away from the decentralised and light-touch philosophy of PM-WANI. On the contrary, **capable and serious system integration layers may actually help preserve and scale the decentralised participation model by allowing local PDOs to remain simple and low-complexity participants** while more sophisticated operational functions are managed centrally or through platform ecosystems.

E. POLICY AND INSTITUTIONAL SUPPORT REQUIRED

E1. Interoperable frameworks and technical standardisation

Policy and institutional support may therefore focus upon the **creation of enabling and interoperable frameworks** rather than highly prescriptive structures. **In this regard, interoperable API standards, standardised backend integration frameworks, common authentication interfaces, roaming interoperability architectures and certification frameworks may significantly improve ecosystem scalability**. Simplified technical integration frameworks may also encourage participation by smaller ISPs and regional providers.

E2. Managed-service enablement and open architecture principles

Institutional support may additionally focus upon the standardisation of interoperability frameworks, managed-service enablement, digital trust and security frameworks, roaming and settlement standards, municipal integration frameworks and provider-neutral infrastructure access models. The ecosystem may also benefit from the development of open and interoperable architecture principles so that multiple competing system integrators can coexist and innovate without creating closed or monopolistic ecosystems.

E3. Bridging telecom infrastructure and local digital ecosystems

Another important consideration is that s**ystem integrators may help bridge the current gap between telecom infrastructure providers and local digital participation ecosystems. Public Wi-Fi proliferation ultimately requires coordination across broadband providers, municipalities, venue owners, local entrepreneurs, App Providers, public institutions and digital platforms. System integrators may therefore function as the operational layer capable of aligning these fragmented stakeholders into commercially viable ecosystems.**

E4. Evolving TSP and ISP participation through managed integration models

The role of TSPs and ISPs may also evolve positively within such frameworks. Rather than viewing Public Wi-Fi as a standalone layer, **scalable system integration ecosystems may enable TSPs and ISPs to participate through managed hotspot services, broadband provisioning, traffic offload arrangements, enterprise integration, roaming**

ecosystems and platform partnerships. This may **create stronger commercial alignment between Public Wi-Fi proliferation and broader broadband ecosystem growth.**

E5. A neutral ecosystem coordination and interoperability framework

In this context, there may also be merit in developing a **neutral ecosystem coordination and interoperability framework** capable of **supporting long-term alignment across PDOs, PDOAs, App Providers, ISPs, system integrators, public institutions and other ecosystem participants.** The objective of such a framework should not be to create a centralised operational monopoly or replace market-led innovation, but rather to **provide trusted and interoperable digital rails upon which competitive ecosystem participants may innovate independently.** Such a neutral framework may support standardisation, interoperability coordination, ecosystem analytics, transparency, roaming evolution, stakeholder engagement and long-term mission alignment while preserving competition and decentralised participation. **A useful reference in this regard may be the manner in which interoperable digital public infrastructure ecosystems such as UPI evolved through neutral coordination layers combined with strong private-sector innovation at the application and service layer.**

Overall, strengthening the role of capable and serious system integrators may become essential for transforming India's Public Wi-Fi ecosystem from fragmented hotspot deployment into a scalable, interoperable and commercially sustainable digital connectivity layer. A balanced framework combining decentralised participation with strong aggregation, managed-service capability and interoperable platform ecosystems may provide the most sustainable pathway for large-scale Public Wi-Fi proliferation in India.

Q22. Are users experiencing challenges with the authentication and authorization procedures for accessing Public Wi-Fi Networks? If yes, how can authorization and authentication processes be simplified while ensuring security and compliance? Please provide your response in detail with justification.

A. AUTHENTICATION FRICTION AS A SIGNIFICANT BARRIER TO PUBLIC WI-FI ADOPTION

Users presently experience significant friction in the authentication and authorisation procedures required for accessing Public Wi-Fi networks in India. In many cases, the onboarding experience remains substantially inferior to the seamless and always-on connectivity experience offered by mobile broadband networks. As discussed in the responses to Questions 1, 2, 5, 6 and 21, this friction represents one of the most significant barriers affecting repeat usage, user trust and the long-term adoption of Public Wi-Fi services.

At present, users are frequently required to undergo repeated OTP-based authentication, download applications, interact with captive portals, activate vouchers and repeatedly re-authenticate across different hotspots. Such fragmented onboarding experiences reduce convenience and create a perception that Public Wi-Fi is cumbersome, unreliable and temporary in nature. Consequently, even where hotspots are available, sustained usage levels often remain limited.

This issue is particularly important because Public Wi-Fi ecosystems compete not merely on affordability, but increasingly on convenience, continuity and overall user experience. If the authentication process itself becomes cumbersome, users are naturally inclined to continue relying on mobile broadband connectivity even in locations where Public Wi-Fi capacity is available. Accordingly, **the long-term objective should be to progressively evolve toward a secure yet nearly invisible authentication experience** comparable to modern broadband and mobility platforms. At the same time, any simplification of onboarding processes must continue to preserve lawful traceability, cybersecurity safeguards, privacy protections and regulatory compliance obligations.

B. KEY MEASURES FOR SIMPLIFYING AUTHENTICATION AND AUTHORISATION

B1. Gradual movement toward persistent and interoperable authentication frameworks

One of the most important requirements is the gradual movement toward interoperable and persistent authentication frameworks. Instead of requiring repeated hotspot-by-hotspot onboarding, users should progressively be able to authenticate once and thereafter experience continuity across participating networks. Technologies such as Passpoint, OpenRoaming and device-based persistent authentication frameworks merit consideration over time because they can enable secure and automated reconnection across interoperable hotspot ecosystems without repeated OTP-based interventions. Such frameworks may significantly improve user convenience, continuity and trust.

At the same time, implementation should remain gradual, interoperable and technology-neutral. India's PMWANI based Public Wi-Fi ecosystem presently consists of highly diverse participants including small PDOs, regional providers, App Providers, institutions and emerging platform ecosystems. Therefore, migration toward seamless authentication should evolve through interoperable standards and scalable backend integration frameworks rather than through rigid or highly centralised architectures.

B2. Layered approach: advanced frameworks combined with inclusive onboarding options

While the long-term evolution of Public Wi-Fi ecosystems may progressively move toward seamless and persistent authentication frameworks such as Passpoint or interoperable

roaming architectures, it is equally important that inclusion-oriented onboarding options continue to remain available during ecosystem evolution. Browser-based and captive-portal-based authentication mechanisms may therefore continue to serve an important role, particularly for first-time users, users with limited-storage devices, low-cost smartphones or digitally less-familiar populations. Accordingly, future authentication frameworks may benefit from a layered approach combining advanced seamless authentication models with simplified browser-based onboarding journeys so that ecosystem scalability and technological evolution do not inadvertently reduce digital inclusion.

B3. Simplified UPI-integrated payment and onboarding flows

Another important aspect relates to the simplification of payment-linked onboarding. Presently, users often encounter multiple steps involving vouchers, application-level payments and fragmented recharge systems. The integration of simplified UPI-based payment flows may substantially improve onboarding ease. Over time, users should be able to discover, authenticate and pay for Public Wi-Fi access through simple, low-friction and interoperable digital flows integrated into commonly accessible applications or platforms.

B4. Trust, security and backend compliance

An equally important issue concerns trust and security assurance. Many users continue to perceive Public Wi-Fi as insecure or vulnerable to misuse. Therefore, simplification of onboarding should not dilute security standards. Instead, backend security frameworks, user isolation mechanisms, encrypted sessions, secure authentication protocols and compliance systems should progressively become stronger even as the visible user experience becomes simpler and more seamless.
Kindly refer to BIF's Note on Trust and Security for Public WiFi networks in Annexure-I .

B5. Interoperability of authentication systems across providers

Another important requirement is the interoperability of authentication systems across providers. Presently, users frequently encounter fragmented ecosystems where different hotspots require different onboarding processes, applications or credentials. This fragmentation weakens continuity and discourages repeat usage. Accordingly, standardised authentication interfaces and interoperable backend architectures may significantly improve ecosystem usability and user confidence. The role of App Providers, PDOAs and system integrators may become particularly important in this regard. As discussed in the response to Question 21, scalable aggregation platforms may help create unified customer interfaces, persistent authentication systems, roaming continuity and backend interoperability across distributed hotspot ecosystems.

B6. Open and provider-neutral interoperability architecture

Another important consideration is that authentication architectures should remain interoperable rather than becoming locked into isolated proprietary ecosystems. Open APIs, common standards and provider-neutral interoperability frameworks may therefore become critical for the long-term scalability and sustainability of the Public Wi-Fi ecosystem.

Overall, the preferred approach should involve a gradual evolution toward secure, interoperable and frictionless authentication ecosystems capable of delivering seamless user experiences while preserving security, traceability and compliance obligations. Such an approach may materially improve user confidence, repeat usage, ecosystem scalability and the long-term adoption of Public Wi-Fi services across India.

Q23. Is there a need for a centralized platform for authentication and payment systems in the Public Wi-Fi ecosystem? If yes, which entity is best suited for its implementation and management? Please provide your response in detail with justification.

A. THE CASE FOR INTEROPERABILITY: FEDERATED RATHER THAN CENTRALISED

There is considerable merit in **developing interoperable and coordinated authentication, settlement and payment frameworks within the Public Wi-Fi ecosystem with participation by serious players who can contribute to the scale required**. However, the preferred approach **should not necessarily involve a rigidly centralised or monopolistic architecture.** Instead, **the long-term objective should be the creation of a federated, interoperable and scalable ecosystem capable of delivering a seamless user experience while simultaneously preserving innovation, competition and operational flexibility.**

At present, fragmentation across authentication systems, onboarding mechanisms, payment flows and hotspot discovery processes creates substantial user friction and weakens interoperability across networks. As discussed in earlier responses, Public Wi-Fi ecosystems currently function more like disconnected hotspot islands rather than a unified broadband access layer. This fragmentation adversely affects user convenience, roaming continuity, repeat usage, settlement efficiency and overall ecosystem scalability. Consequently, there is **clear value in establishing common interoperability and settlement frameworks that can support authentication interoperability, roaming continuity, payment settlement, hotspot discovery and standardised backend interaction across participating entities.**

At the same time, such frameworks should evolve through open and federated architectural principles rather than through a single closed operational monopoly. The ecosystem may therefore benefit more from a neutral interoperability layer or a federated clearing house architecture instead of a highly centralised retail operating entity.

Such a framework can support interoperability among PDOAs, App Providers, ISPs, system integrators and hotspot operators while still allowing healthy competition and innovation at the service layer. The objective should be to create trusted and interoperable digital rails enabling seamless user experience while preserving innovation, competition and operational flexibility among all ecosystem participants. Users should experience Public Wi-Fi as a coherent and interoperable national connectivity ecosystem rather than as fragmented and isolated provider silos, and a federated interoperability framework can support persistent authentication, roaming settlement, interoperable payments, identity exchange and standardised APIs without preventing multiple competing ecosystem participants from innovating independently.

B. THE ROLE AND NATURE OF THE IMPLEMENTING ENTITY

The role of the implementing entity therefore becomes particularly important. The interoperability framework should be operated through a neutral, trusted and standards-based institutional structure capable of maintaining confidence across TSPs, ISPs, PDOAs, App Providers, public institutions and users. Such a framework may be implemented through a neutral industry-led entity, a standards-based consortium, a regulated interoperability framework or a federated institutional architecture involving multiple ecosystem stakeholders.

In this context, the role of Government and regulators should focus on enabling interoperability, establishing standards, promoting open architecture principles, ensuring non-discriminatory access and preventing anti-competitive concentration. At the same time, the operational layer itself should continue evolving through market-driven innovation and platform participation.

C. PAYMENT INTEROPERABILITY, ROAMING AND DISCOVERY FRAMEWORKS

Another critical aspect is payment interoperability. Fragmented payment systems and isolated voucher ecosystems reduce convenience and weaken roaming capability. **Integration with UPI ecosystems and interoperable digital payment frameworks can therefore significantly improve both user experience and settlement efficiency.** Similarly, interoperable hotspot discovery and roaming frameworks will become increasingly important as hotspot density expands. Users should be able to discover, access and move across participating hotspot ecosystems without repeatedly navigating fragmented applications or isolated onboarding systems.

The role of system integrators and aggregation platforms may also become particularly important in operationalising such interoperability frameworks. Scalable system integration ecosystems can help bridge fragmented local deployments into interoperable national-level ecosystems capable of supporting seamless user mobility and service continuity.

Overall, while there is a clear need for stronger interoperability and coordinated authentication and payment ecosystems, the preferred approach should involve the development of a federated, standards-based and interoperable architecture with a limited number of large interoperable aggregation ecosystems rather than a highly centralised monopolistic platform. Such an approach is likely to provide the appropriate balance between seamless user experience, operational scalability, ecosystem innovation, competition and the long-term sustainability of India's Public Wi-Fi ecosystem and will be devoid of risks attached to a centralised platform.

Q24. What steps are required to achieve interoperability and seamless roaming among Public Wi-Fi networks? Should inter-hotspot roaming be made mandatory, and if so, should a "super-aggregator" be introduced to facilitate it? Please provide your response in detail with justification.

A. INTEROPERABILITY AND ROAMING AS CRITICAL LONG-TERM REQUIREMENTS

Achieving interoperability and seamless roaming may become one of the most important long-term requirements for transforming Public Wi-Fi in India from fragmented hotspot deployments into a scalable national broadband access layer. As discussed in the responses to Questions 4, 6, 21, 22 and 23, the future success of Public Wi-Fi ecosystems will depend not merely upon hotspot availability, but upon continuity of user experience, ease of access and interoperability across networks.

At present, Public Wi-Fi ecosystems in India remain highly fragmented. Different hotspots frequently operate through isolated onboarding systems, applications, authentication methods and payment architectures. As a result, users often experience Public Wi-Fi as disconnected and temporary connectivity rather than as a trusted and persistent broadband layer. This fragmentation reduces repeat usage, weakens customer familiarity and limits ecosystem scalability. Accordingly, interoperability and roaming frameworks may become increasingly important as hotspot density and ecosystem maturity evolve.

The long-term objective should be that users can discover, access and move across participating hotspot networks with minimal friction, comparable to the continuity experienced in mobile broadband ecosystems. However, achieving this objective will require gradual development of interoperable authentication systems, standardised APIs, roaming settlement frameworks, hotspot discovery systems, persistent identity management and interoperable payment architectures.

B. STEPS REQUIRED TO ACHIEVE INTEROPERABILITY AND SEAMLESS ROAMING

B1. Open and interoperable technical standards

The role of open and interoperable technical standards will therefore become particularly important. **Interoperability should evolve through common architecture principles and standardised backend integration frameworks may significantly improve compatibility across PDOAs, App Providers, ISPs, system integrators and hotspot operators.** Technologies such as Passpoint and OpenRoaming may also gradually become relevant as the ecosystem matures because such frameworks can support automated authentication, persistent device recognition and seamless reconnection across participating networks. However, implementation should remain phased, practical and inclusive given the diversity of India's Public Wi-Fi ecosystem.

B2. Interoperable settlement and clearing house architecture

Another important requirement is the development of an interoperable settlement architecture. Roaming ecosystems cannot scale sustainably unless participating entities are able to authenticate users, exchange usage information, settle payments and manage trust relationships through standardised backend systems. As discussed in the response to Question 23, this may require development of federated clearing house frameworks or interoperable backend ecosystems capable of supporting multi-provider coordination without creating rigid centralisation.

C. SHOULD INTER-HOTSPOT ROAMING BE MADE MANDATORY?

With regard to whether inter-hotspot roaming should be mandatory, a balanced and phased approach may be preferable. **In principle, interoperability and roaming are highly desirable long-term objectives because they materially improve user convenience, repeat usage, ecosystem scalability and commercial sustainability.** However, the **ecosystem presently remains at a relatively early and heterogeneous stage of development.** Immediate mandatory nationwide roaming obligations may therefore create operational complexity for smaller PDOAs, local providers and emerging ecosystem participants.

Accordingly, a phased approach may be more practical during ecosystem maturation. Participation in interoperable roaming frameworks may initially evolve through voluntary participation, standardised interoperability frameworks, platform aggregation, managed-service ecosystems and market-led partnerships. Over time, as ecosystem maturity improves, interoperability requirements may gradually become more standardised for networks seeking participation in broader Public Wi-Fi roaming ecosystems.

D. SHOULD A 'SUPER-AGGREGATOR' BE INTRODUCED?

D1. The case for aggregation layers

The concept of a super-aggregator requires careful consideration. There may indeed be value in the emergence of strong aggregation and interoperability layers capable of facilitating roaming, supporting settlement, enabling authentication exchange, aggregating hotspot discovery and simplifying user access. However, the **preferred model may not necessarily be a single monopolistic central operator controlling the entire ecosystem, At least two to three SPDOAs could be conceived , so that there is enough competition between them which will lead to improved quality of service at affordable rates.**

D2. A federated aggregation model as the preferred approach

Instead, the ecosystem may benefit more from a **federated and interoperable aggregation architecture where a limited number of serious competing aggregation and platform entities, having certain scale and eligibility, coexist through open standards and interoperable APIs.** Such an approach may preserve innovation, competition, operational flexibility and ecosystem resilience while still enabling a seamless user experience. As discussed in the response to Question 21, strong and serious system integrators, PDOAs, App Providers and managed-service ecosystems may together perform many of the operational roles associated with roaming enablement and interoperability management.

D3. Preserving accessibility for smaller participants

Another important consideration is that interoperability should not inadvertently increase barriers for smaller participants. The Public Wi-Fi ecosystem derives significant strength from its decentralised and low-entry structure. Therefore, interoperability frameworks should remain proportionate, scalable, open and operationally practical. Smaller PDOs and local entrepreneurs should continue to participate without facing telecom-grade operational complexity.

E. ROLE OF GOVERNMENT AND REGULATORS

The role of Government and regulators may therefore focus upon enabling open interoperability standards, encouraging roaming frameworks, supporting common architecture principles, ensuring non-discriminatory participation and promoting ecosystem coordination. At the same time, innovation at the operational and platform layer may continue to evolve through market participation and competitive ecosystem development.

Overall, interoperability and seamless roaming are likely to become essential for the long-term evolution of Public Wi-Fi into a trusted and scalable broadband access layer in India. A phased, federated and standards-based approach combining open interoperability, aggregation ecosystems and competitive platform participation may provide the most sustainable pathway for achieving seamless Public Wi-Fi roaming at national scale.

Q25. What monetisation models are most appropriate for rural, urban, and high-footfall locations, respectively? Please also suggest any additional monetisation models that may be suitable in the Indian context. Please provide your response in detail with justification.

A. THE NEED FOR FLEXIBLE AND ENVIRONMENT SPECIFIC MONETISATION MODELS

The long-term sustainability of Public Wi-Fi ecosystems in India will depend fundamentally upon the emergence of commercially viable, scalable and locally adaptable monetisation models. As discussed in the responses to Questions 3, 4, 7, 8, 18, 19 and 20, Public Wi-Fi proliferation cannot rely indefinitely upon subsidy-driven or purely experimental deployment approaches. Instead, the **ecosystem must gradually evolve into a sustainable digital infrastructure and service layer capable of generating long-term economic value for all participating stakeholders.**

At the outset, it is important to recognise that there is **unlikely to be a single universal monetisation model suitable for all deployment environments.** The economics of Public Wi-Fi differ substantially across rural areas, urban commercial centres and high-footfall public locations because factors such as user density, purchasing power, infrastructure costs, traffic intensity and commercial opportunities vary significantly across these geographies. **Accordingly, the monetisation framework should remain flexible, technology-neutral and commercially adaptive, rather than prescriptive.**

B. MONETISATION MODELS FOR RURAL AND UNDERSERVED AREAS

B1. Community utility and institutional integration

In rural and underserved areas, monetisation models are likely to depend more heavily upon community-level utility, institutional integration and shared access frameworks rather than purely retail consumer usage. In many such areas, standalone hotspot economics may remain weak during the initial stages of deployment due to lower user density and limited monetisation potential. Therefore, sustainability may emerge through integration with broader digital public infrastructure and local service ecosystems.

In this context, Public Wi-Fi in rural areas may increasingly derive value through support for digital education, telemedicine, e-governance access, online service delivery, agricultural information systems, digital payments, Common Service Centre ecosystems and local entrepreneurship initiatives. Accordingly, institution-linked models, shared community access frameworks and managed-service approaches may become particularly relevant in rural environments.

B2. Gradual evolution of rural monetisation

Over time, rural monetisation may improve gradually through increased digital adoption, greater participation in local digital commerce and rising familiarity with broadband-based services among users. The long-term viability of rural models may therefore depend upon progressive community-level ecosystem development rather than immediate commercial returns.

C. MONETISATION MODELS FOR URBAN ENVIRONMENTS

C1. Diverse commercial models and beyond simple retail connectivity

In urban environments, monetisation opportunities are likely to be significantly stronger because of higher population density, concentrated commercial activity, stronger broadband demand and greater opportunities for customer engagement. Urban Public Wi-Fi ecosystems may, therefore, support a much wider variety of commercial models. Traditional prepaid access models and sachet-style usage plans may continue to remain relevant for certain user segments. However, monetisation is likely to evolve beyond the simple retail sale of connectivity. Freemium models, venue-sponsored access, subscription-based access, retail bundling and digital engagement ecosystems may increasingly become important components of urban Public Wi-Fi business models.

C2. Indirect monetisation through local digital commerce and customer engagement

Commercial establishments may particularly benefit from indirect monetisation opportunities where Public Wi-Fi improves customer footfall, customer dwell time, digital engagement and local visibility. Cafes, retail shops, restaurants, malls and other public-facing establishments may increasingly integrate Public Wi-Fi with customer loyalty programmes, digital promotions, purchase-linked access systems and local advertising ecosystems. In this sense, Public Wi-Fi may gradually evolve not merely as a connectivity service, but as a local digital commerce and customer engagement platform. Such models may become especially important in India where neighbourhood commerce ecosystems and small enterprises continue to play a major economic role.

C3. Platform aggregation and interoperable ecosystem development

Another important urban monetisation opportunity lies in platform aggregation and interoperable ecosystem development. As discussed in the responses to Questions 4 and 21, scalable PDOAs, App Providers and system integrators may aggregate thousands of hotspots into unified discovery, billing and roaming ecosystems. Such aggregation may support subscription-based access models, interoperable access packs, digital advertising ecosystems, customer analytics services and broader platform-based revenue opportunities. **The role of App Providers and aggregation platforms may therefore**

become increasingly important in improving commercial viability across fragmented hotspot deployments.

D. MONETISATION MODELS FOR HIGH-FOOTFALL ENVIRONMENTS

High-footfall environments such as airports, railway stations, transport systems, tourism zones, educational campuses, public institutions and dense commercial districts may support even more sophisticated monetisation models because of concentrated demand, repeat usage patterns and higher traffic intensity. Such environments may support premium speed access tiers, venue-integrated connectivity ecosystems, tourism-linked services, transport integration, digital way-finding systems, analytics-driven services and managed enterprise connectivity frameworks. Advertising-supported models and location-based digital engagement ecosystems may also become commercially attractive in such environments due to the scale and predictability of user traffic.

E. ADDITIONAL MONETISATION MODELS SUITABLE IN THE INDIAN CONTEXT

E1. Integration with digital public infrastructure and urban digital services

An additional opportunity may emerge through integration of Public Wi-Fi ecosystems with broader digital public infrastructure and urban digital services. Public Wi-Fi may increasingly support digital payments, e-governance services, tourism information systems, smart mobility platforms, educational access systems, public information services and local digital marketplaces. Such integration may create indirect economic value that extends beyond simple bandwidth monetisation.

E2. Traffic offload and broadband augmentation arrangements

Another important monetisation opportunity may gradually emerge through traffic offload and broadband augmentation arrangements. As discussed in the response to Question 18, interoperable Public Wi-Fi ecosystems may over time support improved network efficiency and enhanced customer experience in dense urban and indoor environments. Commercially negotiated offload arrangements and managed-service participation models may therefore create additional wholesale or partnership-based revenue opportunities in selected environments.

E3. Managed-service and infrastructure-sharing models

The ecosystem may also benefit significantly from managed-service and infrastructure-sharing models. Smaller establishments and institutions may not independently possess the operational capability required to manage hotspot systems effectively. Accordingly, managed-service providers, PDOAs and system integrators may increasingly provide bundled operational frameworks involving connectivity, authentication systems, backend management, customer support, analytics and roaming integration. Such aggregation may

improve commercial viability while simultaneously reducing operational complexity for local participants.

F. REGULATORY APPROACH AND CONDITIONS FOR LONG-TERM MONETISATION SUSTAINABILITY

The monetisation framework should remain sufficiently flexible to accommodate diverse local conditions and evolving technological models. Different stakeholders may participate in the ecosystem for different reasons. Some establishments may seek direct revenue generation, while others may prioritise customer engagement, digital visibility, community service objectives or broader ecosystem participation. **Accordingly, consideration may be given to ensuring that the regulatory approach does not lock the ecosystem into narrow or overly prescriptive commercial structures. Innovation in monetisation models need to continue evolving through market participation, technological innovation and platform development.**

Another important consideration is that long-term monetisation success will depend significantly upon user experience, interoperability and ecosystem trust. Fragmented, low-quality or cumbersome Public Wi-Fi environments are unlikely to generate sustainable commercial adoption regardless of pricing models. **Accordingly, monetisation sustainability is closely linked with improvements in authentication simplicity, roaming capability, service quality, interoperability, hotspot discoverability and overall user confidence.**

Overall, the preferred approach may therefore involve the development of flexible, layered and environment-specific monetisation ecosystems combining direct connectivity revenues, indirect commercial value creation, platform aggregation, managed-service participation, institutional integration, digital commerce opportunities and broader digital ecosystem participation. Such an approach may provide the strongest foundation for sustainable and scalable Public Wi-Fi proliferation across diverse Indian geographies and usage environments.

Q26. Please provide any additional comments, observations, or suggestions related to the proliferation of Public Wi-Fi in the country, including any potential issues or considerations that may not have been covered in the sections above. Please provide your response in detail with justification.

A. VIEWING PUBLIC WI-FI PROLIFERATION AS A NATIONAL BROADBAND ACCESS ECOSYSTEM

A1. Public Wi-Fi as a National Broadband Access Ecosystem

As an **additional overarching submission, it may be useful to view Public Wi-Fi proliferation in India not merely as a hotspot deployment exercise, but as the gradual creation of a scalable and interoperable national broadband access ecosystem.** The long-term success of such an ecosystem is likely to depend upon achieving the right balance between open participation, interoperability, commercial scalability and sustainable investment incentives.

A2. Public Wi-Fi as a Core Broadband Access Layer

Public Wi-Fi may be recognised as a strategic component of India's broadband architecture, complementing both mobile broadband and fixed broadband networks. Its role extends beyond hotspot deployment and includes broadband augmentation, indoor connectivity enhancement, traffic offload, digital inclusion and support for high-capacity digital applications. Public Wi-Fi policy may therefore be aligned with broader national broadband objectives and infrastructure planning initiatives.

A3. Public Wi-Fi as Digital Public Infrastructure

Public Wi-Fi may increasingly be viewed as a foundational digital access layer supporting education, telemedicine, e-governance, digital payments, local commerce, tourism services and future smart-city applications. The long-term value proposition extends beyond internet access alone and includes enabling participation in India's wider digital economy.

B. EMERGING DEMAND FROM WORK FROM HOME AND HYBRID WORK MODELS

B1. Public Wi-Fi as a Neighbourhood Broadband Access Layer

An important **emerging demand side factor is the increasing relevance of Work From Home and hybrid work models.** Over the last few years, remote working has become an important part of urban employment, business continuity, pollution response, fuel conservation and crisis-management strategies. Work From Home materially changes the nature of broadband demand because users require stable, high-capacity and low-latency connectivity for video conferencing, cloud applications, enterprise systems, large file transfers and online collaboration.

B2. Emerging Demand from Education, Digital Livelihoods and Community Connectivity

This has important implications for Public Wi-Fi policy. **Where FTTH penetration remains limited, affordability is a constraint, or residential broadband quality is inadequate, there is a clear role for high-quality Public Wi-Fi access points located in the vicinity of residential clusters, community centres, libraries, local markets, co-working spaces, educational institutions and other neighbourhood-level public or semi-public locations.** Such access points should not be viewed as a substitute for household fixed broadband. Rather, they may function as a complementary neighbourhood broadband access layer, enabling users who do not yet have reliable fixed broadband at home to access stable connectivity for productivity-oriented digital use. This is particularly relevant

for students, gig workers, freelancers, small entrepreneurs and employees who require occasional or regular high-capacity access but may not be able to afford or obtain reliable FTTH connectivity immediately. **Demand side policy should, therefore, recognise that Public Wi-Fi demand is no longer limited to casual browsing or low-value data usage. It increasingly includes productivity, education, remote work, telemedicine, digital governance and livelihood-linked use cases.**

B3. Supporting Productivity, Education and Digital Livelihoods

In addition to Work From Home, Public Wi-Fi demand is increasingly driven by students, gig workers, freelancers, micro-enterprises, digital entrepreneurs and community users requiring affordable access to high-capacity broadband. Public Wi-Fi can therefore serve as an important neighbourhood-level access layer supporting productivity, skill development, digital livelihoods and inclusive participation in the digital economy.

C. EMERGING TECHNOLOGY DIMENSIONS REQUIRING FORWARD-LOOKING POLICY ATTENTION

The CP specifically identifies AI-enabled network optimisation and advanced Wi-Fi sensing as emerging capabilities that will characterise the next generation of Public Wi-Fi ecosystems. These developments merit forward-looking policy attention because they represent a qualitative shift in what Public Wi-Fi infrastructure can do i.e. moving it from a passive connectivity layer to an active and intelligent digital infrastructure platform.

C1. AI-Enabled Network Optimisation and Intelligent Network Management

AI-enabled network optimisation refers to the use of machine learning and data analytics to dynamically optimise channel allocation, interference management, load balancing, predictive maintenance, congestion prediction and quality of service assurance across distributed hotspot networks. Such capabilities can significantly improve the consistency and reliability of Public Wi-Fi service quality without proportionate increases in operational cost. As AI-based network management tools become more accessible and affordable, they may become particularly important for PDOAs and system integrators managing large numbers of distributed hotspots across heterogeneous environments. The regulatory framework should avoid inadvertently restricting data collection and analytics necessary for such network management functions, while ensuring that appropriate user privacy safeguards remain in place consistent with India's data protection framework.

C2. Wi-Fi Sensing and the Evolution of Public Wi-Fi Infrastructure

Wi-Fi sensing represents an even more transformative capability. Modern Wi-Fi standards, particularly Wi-Fi 6E and Wi-Fi 7, enable wireless signals to be used not only for data transmission but for environmental sensing i.e. detecting presence, motion, respiration, falls and other physical events without requiring dedicated sensor hardware. This capability has

significant potential applications in healthcare monitoring in hospitals and elderly care facilities, security and intrusion detection in public spaces, occupancy management in transport hubs and educational campuses, and smart city applications. India, with its large and ageing population and its healthcare infrastructure gaps, represents a particularly compelling environment for Wi-Fi sensing applications. BIF submits that the Authority may consider acknowledging Wi-Fi sensing as an emerging and legitimate use of Public Wi-Fi infrastructure and may recommend that the regulatory framework remain sufficiently technology-neutral and forward-looking to enable such applications to develop without unnecessary definitional or licensing constraints.

C3. Privacy, Consent and Data Governance for Emerging Applications

At the same time, clear guidelines on privacy, consent and data governance for sensing applications may be developed in consultation with relevant authorities as the technology matures.

C4. Wi-Fi 6E, Wi-Fi 7 and Future Spectrum Readiness

Future Public Wi-Fi policy should support migration towards Wi-Fi 6E, Wi-Fi 7 and other next-generation technologies through timely availability of licence-exempt spectrum (eg, V Band), affordable device ecosystems and technology-neutral regulatory frameworks. Such technologies will become increasingly important for supporting high-density connectivity environments and emerging digital applications.

C5. 5G-Wi-Fi Convergence

Future broadband architectures are likely to involve increasing convergence between mobile and Wi-Fi networks. Public Wi-Fi should therefore be positioned as a complementary broadband access technology capable of supporting traffic offload, improved indoor coverage and efficient utilisation of scarce licensed spectrum resources.

D. A LAYERED AND INTEROPERABLE ECOSYSTEM ARCHITECTURE FOR INDIA'S PUBLIC WI-FI

D1. The foundational interoperability layer

The future Public Wi-Fi architecture in India may evolve through a layered and interoperable ecosystem framework. At the foundational level, India may benefit from development of neutral and interoperable digital rails supporting standards, authentication interoperability, roaming continuity, settlement frameworks and ecosystem coordination. Such foundational interoperability layers may function as enabling digital infrastructure supporting seamless user experience and ecosystem-wide compatibility while preserving openness and competition. The objective should not be creation of a monopolistic central operator, but rather establishment of trusted and interoperable digital infrastructure capable of enabling serious ecosystem participants to innovate and scale. A useful reference in this regard may

be the manner in which interoperable digital public infrastructure ecosystems such as UPI evolved through neutral coordination layers combined with strong private-sector innovation at the application and service layer.

D2. The aggregation and managed-service layer

Above this interoperability layer, the ecosystem may gradually witness emergence of competing and scalable aggregation and managed-service ecosystems involving PDOAs, App Providers, system integrators, managed-service providers, ISPs, TSPs and other digital platform participants. Such entities may play a critical role in transforming fragmented hotspot deployments into integrated and commercially sustainable ecosystems by enabling customer discovery, authentication continuity, roaming, settlement, analytics, customer support, digital engagement and large-scale operational management. The emergence of strong and interoperable aggregation ecosystems may also improve investment confidence and create commercially scalable participation opportunities for both telecom and digital ecosystem players.

D3. The distributed local participation layer

At the participation layer, the ecosystem may continue to remain highly distributed and entrepreneur-driven, involving shops, institutions, transport hubs, commercial establishments, community centres, educational institutions, public venues and local PDOs. This decentralised participation structure remains one of the strongest aspects of the PM-WANI based Public WiFi approach because it enables broad-based local participation without requiring telecom-style licensing complexity.

D4. Public Wi-Fi Spatial Planning and Infrastructure Coordination Layer

The proliferation of Public Wi-Fi may benefit from a spatial-planning approach involving hotspot clusters, Wi-Fi zones, Wi-Fi corridors and district-level deployment planning. Rather than isolated hotspot deployment, planning may be aligned with population density, transport networks, educational institutions, healthcare facilities, markets, tourism destinations and underserved communities. Such an approach can improve discoverability, utilisation, sustainability and long-term ecosystem value.

D5. The BharatNet and Shared Infrastructure Layer

The long-term success of Public Wi-Fi proliferation may depend significantly upon deeper integration with BharatNet, State fibre networks, municipal fibre systems, Smart City infrastructure and other public digital assets. Existing fibre assets of RailTel, PowerGrid, utility networks, municipal authorities, cable operators and other infrastructure providers may also be leveraged through commercially negotiated and technically appropriate sharing arrangements. Such integration can materially improve deployment economics and accelerate geographic coverage.

D6. The Managed Participation Layer for Small Enterprises

To encourage large-scale participation by small businesses and community institutions, Public Wi-Fi deployment should progressively evolve towards managed-service models that minimise technical complexity. Standardised plug-and-play solutions, remote management capabilities and simplified onboarding can make participation as easy as adopting digital payment platforms or other digital public infrastructure services.

D7. Leveraging Existing FTTH Infrastructure

A significant opportunity may exist in enabling PM-WANI functionality through existing FTTH deployments. Many broadband ONTs already incorporate Wi-Fi capabilities and, subject to technical feasibility, could support Public Wi-Fi through software upgrades, managed-service arrangements or secondary SSID implementations. Such an approach may substantially increase hotspot density at relatively low incremental cost.

D8. Local Government as Digital Infrastructure Facilitators

Municipalities and Panchayats may increasingly be viewed as digital infrastructure facilitators rather than merely approval-granting authorities. Their role may include hotspot planning, infrastructure access coordination, local demand aggregation, awareness generation, Smart City integration and support for community-level deployment initiatives.

E. THE PREFERRED ARCHITECTURE: FEDERATED, INTEROPERABLE AND MARKET-SCALED

E1. Interoperability Without Centralisation

Accordingly, India's long-term Public Wi-Fi framework may benefit from combining interoperable national digital rails, scalable competitive aggregation ecosystems and distributed local participation within a unified but innovation-friendly architecture. Such an approach may provide the strongest balance between interoperability, investment scalability, competition, innovation, inclusion and long-term sustainability.

E2. Balancing Competition, Innovation and Scale

Overall, the preferred approach may therefore involve avoiding both extremes — namely fragmented isolated hotspot ecosystems on one hand and excessively centralised monopolistic operational structures on the other. Instead, India may benefit most from a federated, interoperable and market-scaled Public Wi-Fi architecture capable of evolving into a trusted national broadband augmentation layer supporting digital inclusion, broadband growth and future digital infrastructure expansion.

E3. Sustainable Funding and Market Development

Public funding, where required, may be targeted towards market-failure situations, underserved geographies and ecosystem development objectives. Funding frameworks may increasingly focus on usage, uptime, service quality and sustainability outcomes rather than deployment numbers alone, while preserving long-term market incentives and commercial viability.

E4. Strengthening Participation of ISPs, TSPs and Digital Ecosystem Players

The long-term success of Public Wi-Fi proliferation will depend upon active participation by ISPs, TSPs, PDOAs, App Providers, system integrators and managed-service providers. Policy frameworks may encourage traffic-offload arrangements, infrastructure sharing, managed hotspot services and platform-based innovation that align Public Wi-Fi growth with broader broadband ecosystem development.

WiFi security

In WiFi a technique known as Wired Equivalent privacy (WEP) was used in the first version which has used a stream cipher using RC4 algorithm[1]using a key of 40 bits or 104 bits .and an initialization vector (IV) of 24 bits makes up overall key of 64 bits (or 128 bits). Note that initially the WiFi device and access point (AP) have preshared key installed. All the WiFi devices share the pre-shared key (PSK) with the AP. Several attacks such as collision attack, chop-chop attack are available openly in *Aircrack-ng* and *John the Ripper*.

The next generation Wi-Fi protected access (WPA)[2]also was shown to be vulnerable for attacks and was replaced in Wi-Fi Protected Access (WPA2) protocol which uses stronger AES-CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) encryption algorithm. WPA2-PSK needs proper passphrase at least 16 characters so that the time needed to crack that password is measured in decades, not hours.

Note that WPA-2 is available in two modes: WPA2-*personal* and WP2-enterprise. Note that the WPA2-*personal* uses pre-shared key discussed above. On the other hand, deploying WPA2-Enterprise requires a RADIUS (*Remote authentication dial-in user service*) server (also called AAA (Authentication, Authorization and accounting) server). Note that X.509 digital certificates are used for authentication[3]. WPA2 Enterprise requires an 802.1X authentication server.

WPA2 uses four-way handshake shown which needs the existence of Pre-Shared Key (PSK) without actually transmitting it. During this handshake, a Pairwise Transient Key (PTK) and Groupwise transient key (GTK) are generated for secure data exchange using MAC addresses, nonces and SSID (Service set identifier which can be seen in the mobile by selecting WiFi settings). Key reinstallation attack (KRACK) was discovered forcing nonce reuse[4]. The KRACK attack can be remedied by checking whether key already in use is being reinstalled. The replay counters and nonces shall not be reset. Some patches have been released and are available. Since WPA2 which was in use for over a decade, WPA3 was introduced in 2018 which solves the problem of offline dictionary attack. WPA3 has two methods: WPA3-SAE, or *Simultaneous Authentication of Equals*. Note that SAE uses *dragon fly Key exchange*[5] and is more resistant to offline dictionary attacks. The end user will not notice any difference since he/she still enters a passphrase on his/her device to secure their Wi-Fi Connections. WPA3-SAE uses *Elliptic Curve Cryptography* (ECC) without needing to send any part of the keys over the air that attackers can capture and then reverse engineer. Note that pairwise master key is based on random numbers and not passwords alone. WPA3 uses AES- CCMP (counter mode with cipher block chaining) and has *forward secrecy* feature which prevents decryption of previous sessions in case current keys are compromised. However, just like with previous generations, not every device today supports WPA3. WPA3 is backward compatible with WPA2 as well as mixed mode WPA2/WPA3 devices.

---

1 M. Shin, J. Ma, A. Mishra and W. A. Arbaugh, "Wireless Network Security and Interworking," in Proceedings of the IEEE, vol. 94, no. 2, pp. 455-466, Feb. 2006, doi: 10.1109/JPROC.2005.862322

2 E. Tews and M. Beck, "Practical attacks against WEP and WPA," in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec '09), Zurich, Switzerland, 2009, pp. 79–86.

3 Simplifying WPA2-Enterprise and 802.1x, Secure W2, https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplif…

4 Mathy Vanhoef and Frank Piessens. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In CCS

5 RFC 7664: Dragonfly Key Exchange, RFC Editor, https://www.rfc-editor.org/rfc/rfc7664.html

Note that *WPA3 Enterprise* version allows individual keys for each user of 192 bits and uses authenticated encryption based on AES –GCMP (Galois counter mode protocol). It also uses 384 bit HMAC (Hashed Message Authentication code) using SHA 384. The key establishment uses 384 bit ECDH (Elliptic Curve Diffie-Hellman key exchange) for key establishment and authentication uses ECDSA (Elliptic Curve Digital Signature Algorithm). Several versions of WPA3 are available (a) WPA3 transition mode (b) WPA3 Easy Connect (c)WPA3 Certified enhanced open and Opportunistic Wireless Encryption.
Attacks on WPA3.

Since the PMK derived for WPA3 is not solely dependent on passphrase but also needs the random scalar and Finite Field Element, WPA3 helps mitigating Offline dictionary attacks where an attacker uses a dictionary of passphrases on a passively observed WPA3-Personal key exchange to obtain the correct passphrase. Even if the attacker was able to obtain the correct passphrase, it only works for the particular session and not other sessions as the PMK changes for other sessions with random numbers used in generating of scalar and Finite Field Element. Other attacks possible are Denial of Service (DoS) Attacks and Disconnect Attacks. WPA3 uses Protected Management Frames which enforces the encryption of frames and enables APs and clients to detect forged disconnect frames and ignore them.

Dragonblood vulnerabilities are a group of security weaknesses identified in the WPA3 Wi-Fi security protocol, particularly affecting its Simultaneous Authentication of Equals (SAE)handshake mechanism , also known as the “Dragonfly Handshake,” which is used in WPA3 for password-based authentication. Dragonblood vulnerabilities can be fixed by installing **latest software patches**, **use of strong passwords on their networks**. The client should remember if a network supports WPA3-SAE also. **The APs deployed in public WiFi must not have option of downgrading to WPA2 and APs with only WPA3 must be made mandatory for public WiFi.**

Another defense, which requires no software patches, is to deploy separate WPA2 and WPA3 networks with different passwords.

Further, UPI and RBI have already issued guidelines to UPI Apps and Banks for deployment of the security architechture [6] [7]. Accordingly, UPI **and banks use HTTPS to encrypt sensitive data, prevent tampering, and ensure you are actually talking to the real bank or UPI-app, not an impostor. Financial sector also uses Multifactor authentication for additional security.**

Therefore, the transactions on the public WiFi are largely secure due to combined effect of WPA3 deployment in the WiFi APs, use of strong password, installation of updated software patch, and use of HTTPS.

PMWANI on top of above employs several safeguards for stronger WiFi login systems. Unlike traditional "open" public Wi-Fi, PM-WANI uses a four-tier architecture with registered Public Data Office Aggregators (PDOAs) and a Central Registry managed by C-DOT, which enforces security standards and mandatory user authentication via mobile verification. The User Authentication & KYC is done through the generation of a fully encrypted token by the PM-WANI App to the AAA server (back-end infrastructure at the PDOA /App Provider’s network).

6 https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2025/07/unified-payments-interface-upi-information-security-compliance-framework-2025.pdf
7 https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721

Upon receipt of Authentication, again in the form of an encrypted token, the App Provider passes the token back to the PDO and the Registration process is thus completed.

Registration/Authorisation of the chosen data tariff plan is also done similarly through the payment gateway (which is part of the backend infrastructure of the App Provider/PDOA) in a completely encrypted fashion.

The framework mandates advanced encryption and secure user authentication, which proponents argue creates a safe environment for sensitive tasks like financial transactions.

Since the WANI Architecture is inherently end-to-end encrypted, there is no question of lack of confidentiality or privacy.

The PM-WANI framework incorporates several layers of encryption and technical standards to ensure that its "distributed" nature doesn't compromise security.

At technical level, the privacy and security in PM-WANI framework is taken care by incorporating two modifications in PMWANI framework and released as PM-WANI V2.0 at the start of 2021.

a) MAC Randomization – PMWANI V1.0 framework was relying on MAC address of the devices to providing internet connection over PMWANI hotspots. MAC addresses are unique identifies of the User Equipment (UE) or device (e.g., Laptop, Smartphones, tablets etc.). The Wi-Fi hotspots may capture these MAC addresses to develop User profile and able to track the user. This puts the User privacy at risk.

   Latest Operating systems (Android, iOS, Windows, Linux) introduced something called MAC Randomization. With this feature enabled (mostly by default), the device exchanges a pseudo-MAC address (and not its actual MAC address) to the Wi-Fi network while browsing internet.

   PMWANI V2.0 specifically addressed this concern and removed the dependency of user device MAC address for the authentication to the network.

These measures are already mandated in PMWANI V2.0 framework guidelines published since 2021.

1. Wi-Fi Access Layer (WPA3)

Modern PM-WANI compliant access points are designed to support WPA3 (Wi-Fi Protected Access 3), the latest industry-standard security protocol, wherever implemented..

Protection against Guessing: It provides robust protection against "brute-force" dictionary attacks, even if a user chooses a weak password.

Individualized Encryption: It uses SAE (Simultaneous Authentication of Equals) to ensure that even if one person's connection is compromised, others on the same network remain private.

2. Authentication & Data in Transit (TLS 1.2/1.3)

Communication between your device, the App Provider, and the PDOA (Aggregator) is secured using Transport Layer Security (TLS), typically versions 1.2 or 1.3.

Encryption Standard: It uses AES (Advanced Encryption Standard) with 128-bit or 256-bit keys to scramble data as it travels.

Integrity Checks: Hashing algorithms like SHA-256 ensure that the data cannot be tampered with or modified during transmission.

Secure Certificates: All entities (App Providers, PDOAs) must use valid SSL/TLS certificates to verify their identity to the Central Registry managed by C-DOT.

3. Identity Verification (KYC & OAuth 2.0)

The framework moves away from the "open" model where anyone can join anonymously.

Mobile OTP KYC: Users must undergo mandatory KYC via Mobile OTP before they can access the network.

OAuth 2.0: This is a standard for secure, token-based authentication that allows you to log in via the PM-WANI app without sharing your actual credentials with the Wi-Fi owner.

4. Backend & Storage Security

The Department of Telecommunications (DoT) has mandated strict data handling for providers:

Data Residency: All user logs and data must be stored within India to comply with national security and privacy laws.

Encryption at Rest: Databases maintained by providers are often encrypted using AES-256 to protect stored user information from unauthorized access.

The PM-WANI framework incorporates multiple layers of authentication, encryption and security controls apart use of APS with standard WPA3 protocols.

Modern financial applications rely primarily on end-to-end application-layer encryption and secure authentication mechanisms, which remain effective across both mobile and WiFi networks including PMWANI.

Further, client separation (also referred to as client isolation or AP isolation) be enabled by default on public Wi-Fi, guest Wi-Fi, and other shared wireless access networks where peer-to-peer communication between user devices is not operationally required. Client separation allows end-user devices to access the internet and communicate with the access point, while preventing direct device-to-device communication on the same Wi-Fi segment. This materially reduces the risk of lateral attacks such as device scanning, ARP spoofing, session hijacking attempts, and unauthorized access between users connected to the same hotspot.

Accordingly, it may be considered that Wi-Fi deployment guidelines, especially for public access and PM-WANI-type environments, should encourage or mandate client separation as a baseline security control.

Thus, for Public WiFi APs following must be mandated :

1. That downgrade from WPA3 to WPA2 is not allowed.
2. Use of Strong Password for network
3. Client separation
4. Timely installation of latest software
5. All Banking and UPI websites and Apps are HTTPs enabled
6. Multifactor authentication for financial transaction
7. Security audit