To,
Shri Neeraj Mittal
Secretary, Ministry of Communications
Government of India

14th August, 2025

In Re: Submission of Comments from Public on The *Draft National Telecom Policy (NTP), 2025*.

Respected Sir,

This letter is in reference to the circular issued by the Department of Telecommunications, Ministry of Communications, Government of India, inviting comments from the public on the Draft National Telecom Policy (NTP), 2025. In furtherance of our commitment to contributing to the legal, regulatory, and technological discourse in the country, and working for public welfare in the capacity of law students, the team at the Cell for Law and Technology ("CLT"), National Law Institute University, Bhopal, hereby submits its suggestions in response to the draft policy.

At the outset, we would like to express our appreciation for this forward-looking initiative to seek public participation in shaping the future of India's telecom sector. This inclusive and consultative approach to policy formulation will help create a balanced, transparent, and effective framework for strengthening digital infrastructure, promoting innovation, and ensuring equitable access to connectivity. As telecommunications continues to underpin India's economic growth, social development, and technological advancement, adopting robust and future-ready strategies will be crucial to addressing sectoral challenges, enhancing resilience, and fostering competitiveness.

The proposed draft has been thoroughly analyzed, and the CLT team has identified a number of key points for consideration, which we have compiled as detailed comments under each mission of the policy. We hope these submissions will contribute meaningfully to the ongoing discussions on creating a strong, secure, and inclusive telecom ecosystem in India.

Thank you for your consideration.

Warm Regards,

Dr. Atul Kumar Pandey
(Professor of Cyber Law; Head, Department of Cyber Law; Faculty in Charge, Cell for Law and Technology)

The team which has been instrumental in putting forward this suggestion comprises of the following members of the Cell for Law and Technology, NLIU Bhopal:

1. Hansika Kumari (Joint Convener) (Final Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
2. Samrudhi Memane (Joint Convener) (Final Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
3. Ashmit Chauhan (4th Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
4. Pheoli Manvind (4th Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
5. Suvansh Shanker (4th Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
6. Khushi Dhingra (4th Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
7. Ayush Murmu (3rd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
8. Prabhash Shukla (3rd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
9. Raj Rajeshwari Meena (3rd Year B.Sc.LLB. (Hons.) Student, NLIU Bhopal)
10. Rujuta Bapat (3rd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
11. Yash Singh (3rd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)

COMMENTS ON THE
DRAFT NATIONAL TELECOM POLICY, 2025

MISSION 1

Strategy No.	Provision	Issues Identified	Proposed Solutions
(1)	1.1 Devise Digital Bharat Nidhi (DBN) schemes to expand mobile network in underserved rural, remote, and urban areas	1. Extremely remote or low-density regions remain unserved due to cost inefficiency. Telecom companies may still avoid areas with extremely low populations. 2. Operators have concerns about DBN fund utilisation and insufficient focus on R&D. 3. Coordination gaps between DBN initiatives and service providers hinder effective rollout.	1. To maximize impact, we recommend that DBN allocations follow a transparent and need-based model, prioritizing regions with the highest connectivity deficit. Clear and detailed guidelines on permissible fund usage should be issued to avoid misuse and ensure alignment with operators' network expansion plans. 2. In geographically challenging regions, such as hilly and remote areas, conventional power supply for mobile towers is often unreliable. Here, solar-powered tower solutions should be actively promoted under the DBN framework to ensure continuous operation. 3. Additionally, public–private partnerships can be encouraged to share risks and resources, thereby improving project viability. To

			expedite implementation, a single-window clearance system, preferably through an online portal, should be adopted to fast-track approvals and reduce bureaucratic delays.
	1.2. Introduce incentive schemes for proliferation of fixed line broadband	1. High capital expenditure discourages private sector investment in fixed-line broadband. 2. Last-mile connectivity remains a bottleneck. 3. Low awareness slows consumer adoption.	1. We recommend that the Ministry consider targeted financial incentives or subsidies for last-mile Internet Service Providers (ISPs), with priority given to regions with minimal fixed-line penetration. 2. Mandating infrastructure sharing, such as poles, ducts, and fiber routes, can substantially reduce deployment costs and accelerate rollout. To stimulate demand, public awareness campaigns should highlight the advantages of fixed-line broadband, especially for education, telemedicine, and e-governance services. 3. Additionally, innovative adoption models can be explored, such as bundling fixed broadband with TV/OTT packages to enhance value for consumers, deploying community broadband hubs (e.g.,

			at panchayat halls) in areas where individual household connections are not immediately feasible, and offering free installation for low-income households to lower entry barriers.
	1.3. Facilitate high-speed radio links for last-mile broadband connectivity	1. Spectrum congestion and interference, especially in densely populated or industrial regions, may reduce link quality. 2. Line-of-sight limitations in hilly, forested, or densely built-up areas can cause signal drops, while adverse weather conditions (heavy rain, storms, dust) may disrupt service reliability. 3. In addition, high capital and operational costs in difficult geographies can deter private investment, and limited technical expertise in rural areas may slow maintenance and fault repair.	1. To address these issues, the Ministry could allocate dedicated spectrum bands for rural last-mile connectivity to reduce interference, and promote cost-effective technologies such as Fixed Wireless Access (FWA) for smaller population clusters. 2. In challenging terrains, government subsidies can encourage private sector participation. 3. Further, using multiple shorter towers instead of a single large link can bypass line-of-sight obstacles, and deploying weather-resistant equipment will improve reliability. 4. A hybrid approach, combining radio links with fiber where feasible, would create a more resilient network. 5. Finally, training local technicians can ensure faster repairs and reduce downtime.

	1.4. Achieve broadband coverage in all inhabited areas using combination of suitable technologies;	1. Integration of diverse technologies presents interoperability challenges that can affect network quality and user experience. 2. Infrastructure gaps in remote villages, coupled with the high cost of certain technologies (e.g., satellite internet) and limited availability of skilled maintenance staff, may hinder effective implementation. Coordination among multiple service providers and technology partners also remains a challenge.	1. The Ministry could facilitate the adoption of national interoperability standards to ensure smooth functioning across different technologies and operators. 2. A district-level technology mix deployment plan should be developed, mapping the most cost-effective combination for each region. 3. Targeted subsidies may be offered for high-cost technologies in extremely remote locations, ensuring no area is left unserved due to economic unviability. 4. Additionally, training local youth in basic network maintenance can improve service reliability and reduce downtime in underserved areas. Close coordination between central and state agencies, supported by a unified monitoring platform, will further strengthen execution and minimize overlaps or delays.
	1.5. Align National Broadband Mission (NBM) to address deployment challenges	1. Fragmented coordination between central, state, and local authorities delays approvals and RoW (Right of Way) clearances.	1. Establish a single-window clearance system under NBM integrating central, state, and local authority approvals for faster

		2. Lack of uniform RoW policies across states results in inconsistent charges, timelines, and conditions for broadband deployment. 3. Inadequate last-mile infrastructure in rural and remote regions leads to slow or stalled project execution. 4. Insufficient monitoring and accountability mechanisms for meeting NBM's annual targets.	decision-making. 2. Create a uniform national RoW policy with standard charges, approval timelines, and guidelines, binding on all states and UTs. 3. Set up a centralised NBM dashboard with state-wise progress tracking, periodic audits, and public disclosure of deployment status. 4. Promote use of innovative, low-cost technologies like aerial fibre, satellite broadband, and community Wi-Fi to bridge last-mile gaps.
	1.6. Leverage BharatNet to fiberize towers and connect public institutions	1. Right-of-Way (RoW) delays – Even though BharatNet fiber passes through many areas, permissions to connect it to towers or institutions often get stuck due to state or local authority delays. 2. Mismatch between fiber route and tower locations – In some places, BharatNet fiber is physically too far from existing towers, requiring costly extensions. 3. Underutilization due to poor backhaul management – Even where fiber is connected, lack of proper backhaul capacity	1. Map fiber routes and tower locations on a single GIS platform to identify and bridge gaps quickly. 2. Pre-negotiate RoW clearances with state governments to avoid case-by-case delays. 3. Install hybrid power solutions (solar + battery) at fiberized sites to reduce downtime. 4. Upgrade backhaul capacity in high-demand areas before traffic congestion becomes an issue. 5. Standardize last-mile equipment and wiring for government offices to ensure quick connection once

		planning means it doesn't improve performance. 4. Electricity reliability issues – Fiberized sites still suffer downtime if the power supply is unstable. 5. Inconsistent last-mile link to institutions – Many government offices have the fiber cable nearby but no proper internal wiring or equipment to use it.	fiber reaches the location.
	1.7. Utilize Optical Ground Wire (OPGW) from the power sector for remote/hilly regions	1. Limited OPGW coverage in non-electrified or poorly electrified areas – Remote villages without high-voltage transmission lines nearby won't benefit from this approach. 2. Aging power infrastructure – In some regions, existing transmission lines are too old or unsafe to retrofit with OPGW. 3. Disruption risks during power line maintenance – Internet services can be interrupted when power lines undergo repair or replacement. 4. Different priorities between sectors – Power companies focus on electricity reliability, not telecom uptime, so OPGW	1. Prioritize OPGW deployment along electrified corridors that align with telecom coverage gaps to ensure maximum benefit. 2. Upgrade old transmission lines in high-priority areas before adding OPGW. 3. Include telecom maintenance clauses in power sector contracts to ensure quick OPGW fault resolution. 4. Use aerial drones for inspection in difficult terrain to speed up repairs. 5. Plan joint deployment during new power projects so OPGW is built in from the start.

		maintenance may not always be timely from a telecom perspective. 5. Challenging terrain access – In hilly regions, reaching power line routes for OPGW installation or repair can be slow and costly.	
	1.8. Map telecom assets on PM GatiShakti NMP and develop GIS-based planning tools	1.Lack of comprehensive, up-to-date mapping of existing telecom infrastructure leads to duplication of efforts and missed opportunities for infrastructure sharing. 2.Inconsistent data formats and absence of real-time updates reduce the accuracy and usefulness of GIS-based planning tools. 3.Limited coordination between telecom operators, local bodies, and infrastructure ministries delays integration of telecom asset data into PM GatiShakti NMP.	1.Mandate all telecom service providers (TSPs), infrastructure providers, and government agencies to upload accurate, standardized, and periodically updated telecom asset data to PM GatiShakti NMP. 2.Develop a unified GIS-based telecom planning platform that integrates layers such as optical fibre networks, mobile towers, small cells, ducts, and satellite gateways, linked with other infrastructure layers (roads, railways, utilities). 3.Provide APIs for private players and state governments to feed real-time updates into the platform, ensuring dynamic and actionable data for planning.
	1.9. Enhance CBuD App for underground	1. The current lack of a comprehensive and updated	1. we recommend integrating all utility providers (including

	infrastructure coordination	database of underground utilities, coupled with limited coordination among multiple utility providers, continues to cause avoidable disruptions. 2. The absence of real-time data further slows down project execution and increases costs.	telecom operators, electricity boards, water supply agencies, and gas companies) into the CBuD platform to ensure a single, authoritative source of information. The platform should be upgraded to enable automated, real-time data sharing, reducing manual intervention and ensuring accuracy. 2. Additionally, regulations should mandate the use of CBuD for all new telecom and utility projects, making compliance a precondition for project approval. 3. On-ground, we note that many local contractors currently do not use such applications due to low awareness and training gaps. There is also incomplete mapping of existing utilities in several districts. To overcome this, we suggest digitizing all underground utility maps in a standardized format and linking them with the CBuD system. 4. Further, targeted awareness and capacity-building drives for contractors and municipal bodies will help ensure that the platform is actively and effectively used.

	1.10. Enable light-touch authorization for submarine cable infrastructure for domestic connectivity	1. The approval process remains lengthy and fragmented, involving multiple agencies with overlapping mandates. 2. Environmental and security clearances, in particular, face significant delays, and the lack of clearly defined regulatory jurisdiction further slows project execution. 3. In addition, security concerns regarding foreign operators and the high capital cost of cable-laying vessels pose additional barriers.	1. We recommend that the Ministry establish a single-window clearance system for all approvals related to submarine cable projects, with clearly defined roles and responsibilities for each regulatory body. 2. Environmental and security assessments should be fast-tracked, with pre-approved routes in environmentally safe zones to reduce procedural delays. 3. To encourage domestic participation, targeted incentives for Indian cable-laying projects could be introduced, which would also help address security considerations and reduce dependence on foreign operators.
	1.11. Promote hybrid access (Mobile, FWA, FTTH, Satellite, Wi-Fi, HAPS, etc.)	1. They present technological complexity and interoperability challenges due to the use of diverse platforms. 2. The cost of deploying and maintaining such a multi-technology ecosystem is significantly higher than single-technology deployments, and quality of service (QoS) can vary across technologies.	1. It is recommended that the Ministry develop unified national standards and protocols to ensure seamless interoperability between access methods. 2. Subsidized pilot projects in rural and underserved regions could demonstrate the viability and cost-effectiveness of such models before large-scale rollout. 3. Additionally, QoS regulations should be tailored to hybrid

			networks, considering the inherent performance differences across technologies.
	1.12. Explore the feasibility of community Wi-Fi networks	1. Community Wi-Fi networks have the potential to offer low-cost internet in underserved regions, but uncertain business models raise sustainability concerns. Ongoing security risks and a lack of local technical capacity further limit adoption.	1. The Ministry could provide seed funding under schemes like Digital Bharat Nidhi and pair it with capacity-building programs for local operators. 2. Robust security protocols, combined with community awareness campaigns, will help build trust in such networks. Partnering with local bodies, cooperatives, and NGOs can ensure smoother operations, maintenance, and community engagement.
	1.13. Promote public Wi-Fi in tourist/public areas and affordable tariffs for PDOs under PM-WANI	1. Public Wi-Fi under PM-WANI can boost digital access in public spaces, but inconsistent coverage and speeds reduce user trust. 2. High tariffs in some areas hinder affordability, and Public Data Offices (PDOs) face difficulty generating sustainable revenue.	1. The Ministry may consider incentivizing deployments in high-footfall tourist and transport hubs and implementing tariff regulation mechanisms to ensure affordability for end-users. 2. Further, revenue-sharing models between PDOs and local authorities, along with training programs on network management and cybersecurity, will enhance operational viability and service quality.

(2)	2.1. Facilitate transition to Network Virtualization and Software-Defined Network (SDN)	1. The transition to SDN brings scalability challenges, particularly with centralized controllers that can become single points of failure. 2. Large SDN deployments add complexity to monitoring and troubleshooting, while controller vulnerabilities present significant security risks. 3. Integration with legacy systems is often difficult, and IT staff require new skill sets to manage the technology effectively.	1. Introduce controller redundancy and high-availability mechanisms to reduce the risk of outages. 2. Invest in advanced monitoring, AI-driven network analytics, and automated fault detection tools for large deployments. 3. Implement robust security frameworks with end-to-end encryption, strict access controls, and real-time threat detection to address vulnerabilities. 4. Launch national-level IT upskilling programs in SDN/virtualization, with a focus on Tier-2 and Tier-3 cities to ensure skill availability nationwide. 5. Follow a phased migration strategy where legacy and SDN systems run in parallel until stability is proven, particularly for mission-critical services like emergency networks.
	2.2. Encourage scalable, programmable architectures for massive IoT	1. The proliferation of devices can lead to network congestion, especially in areas where mobile networks are already overloaded. 2. Interoperability is another barrier, as IoT devices often use different protocols and	1. Develop and adopt open, scalable IoT protocols and standards, mandating interoperability for all licensed device vendors. 2. Introduce a national IoT security certification program to

		proprietary ecosystems, leading to vendor lock-in. Security is a major concern, unsecured IoT devices can be exploited for data theft or botnet attacks. 3. Rural areas also face challenges in deploying IoT at scale due to inconsistent power supply and low local technical capacity.	ensure devices meet minimum encryption and privacy standards. 3. Promote edge computing nodes in rural areas to process IoT data locally and reduce network load. 4. Provide incentives for domestic manufacturing of interoperable IoT devices to reduce costs and dependency on imports. 5. Partner with local training institutes to build IoT maintenance skills at the district level.
	2.3. Support edge computing and cloud integration for AR/VR, smart factories, and autonomous vehicles	1. Emerging applications such as AR/VR, Industry 4.0 manufacturing, and autonomous vehicles require ultra-low latency and high bandwidth, which are difficult to achieve in India's current mixed-quality network environment. 2. Seamless integration between edge computing infrastructure and centralized cloud systems is still in its early stages, and high deployment costs deter private investment. 3. Energy consumption for edge nodes and data centers adds to operational costs, while data sovereignty and privacy are major concerns for sectors handling	1. Release dedicated spectrum for low-latency industrial and AR/VR applications to ensure performance reliability. 2. Encourage standards for hybrid cloud–edge architectures, with interoperability as a priority. 3. Offer financial incentives for green, energy-efficient infrastructure in data centers and edge nodes. 4. Enforce strict data protection and localization requirements for sensitive sectors, combined with localized edge processing to reduce dependence on foreign cloud facilities. 5. Prioritize public–private partnerships to deploy edge

		sensitive information. 4. Rural manufacturing clusters and smaller industrial zones often lack the basic fiber and power backbone to adopt such systems.	infrastructure in smaller industrial towns, ensuring balanced development beyond metropolitan areas.
	2.4. Prioritize release of spectrum for IMT, mmWave, and sub-THz for 6G	1. India already faces spectrum scarcity and allocation disputes between different services such as defense, broadcasting, and telecom. 2. For mmWave and sub-THz bands, which are essential for 6G, technical limitations like poor range and wall penetration make nationwide deployment challenging, particularly in dense urban areas and remote rural geographies. 3. Device and infrastructure costs for these bands remain prohibitively high, and the ecosystem of compatible devices is still developing. In addition, state-level permissions for tower installations and right-of-way can delay deployment timelines.	1. Implement transparent, phased spectrum allocation with extensive industry and stakeholder consultations to avoid conflicts. 2. Fund R&D in advanced antenna systems, beamforming, and propagation technologies to address range and penetration issues. 3. Provide incentives and subsidies to accelerate availability of affordable mmWave/sub-THz devices in the domestic market. 4. Encourage spectrum sharing and dynamic spectrum access frameworks to optimize use of scarce resources. 5. Harmonize central and state regulatory processes for faster network rollouts in both urban and rural areas
	2.5. Align NTN policy with Indian Space Policy 2023 to enhance satellite	1. The separation of terrestrial and non-terrestrial regulations creates fragmentation, making licensing complex and	1. Develop a unified regulatory framework between DoT and space agencies to streamline licensing and reduce duplication.

	communications	international coordination challenging. 2. High infrastructure and terminal costs further hinder adoption.	2. Establish a single-window clearance system for satellite communication projects. 3. Promote public–private partnerships for satellite deployment, focusing on coverage in unserved/underserved regions. 4. Support domestic manufacturing of satellites and user terminals under Make in India to reduce dependency on imports. 5. Encourage Ground Station as a Service (GsaaS) adoption to make satellite access more affordable for smaller operators.
	2.6. Enable Ground Station as a Service (GsaaS) from India	1. High capital costs for ground station infrastructure and a shortage of skilled personnel make widespread adoption difficult. 2. Regulatory and security compliance requirements add further complexity.	1. Government incentives in the form of subsidies and tax benefits should be offered to encourage investment. 2. Specialized training and certification programs can address the skills gap, while clear security guidelines must be developed to balance openness with national security. 3. Develop clear security and regulatory guidelines to balance openness for business with protection of national interests. 4. Facilitate international partnerships for technology

			transfer and capacity building in GsaaS operations.
	2.7. Set up SATCOM Use Case Labs for socio-economic applications	1. High setup and operational costs – SATCOM labs require significant investment in equipment, spectrum licensing, and skilled personnel, which may limit scalability. 2. Limited awareness and adoption among target sectors – Many stakeholders in agriculture, healthcare, and rural development are unaware of SATCOM capabilities.	1. Establish SATCOM Use Case Labs in collaboration with ISRO, DOT, MeitY, and leading academic/research institutions to serve as innovation hubs. 2. Provide dedicated funding and viability gap support for lab setup in rural and aspirational districts. 3. Create a national SATCOM innovation challenge to crowdsource and pilot high-impact use cases in socio-economic domains. 4. Develop standardized interoperability guidelines and compliance frameworks for SATCOM-enabled solutions. 5. Simplify regulatory approvals for experimental SATCOM services and fast-track spectrum allocation for pilot projects.
	2.8. Promote sharing of SatCom networks for affordable, ubiquitous access	1. Coordinating among multiple stakeholders can be difficult, and shared networks raise security and privacy concerns. 2. There is also a risk that a few providers could dominate the market.	1. Transparent sharing frameworks with clear service-level agreements (SLAs) should be developed, incorporating strong encryption and access controls. 2. Competition must be promoted through multi-provider

			ecosystems, and government-backed consortia can be enabled to ensure fair participation.
	2.9. Strengthen India's international engagement (e.g. ITU) to secure orbital slots and ensure spectrum sustainability	1. Scarcity and Competition for Orbital Slots and Spectrum: Orbital slots and radio-frequency spectrum are finite global resources essential for satellite operations. With over 8,000 active satellites and many more planned, intense competition exists internationally for these slots and spectrum bands, leading to scarcity and potential conflicts. 2. Interference and Space Sustainability: Ensuring that satellite operations are free from harmful interference is critical, as is managing orbital traffic to maintain a safe and clean space environment. Increasing satellite congestion increases risks to assets and challenges sustainable operations.	1. Proactive International Engagement: Strengthening India's participation in ITU activities (e.g., World Radiocommunication Conferences) to advocate for increased spectrum allocations and orbital slot rights aligned with technological advances. Active diplomacy to secure favorable spectrum assignments and safeguard interests is key. 2. Collaborative Spectrum Management: Implement cooperation efforts with international agencies (e.g., ITU and European Space Agency) for satellite monitoring, interference resolution, and adherence to shared space sustainability goals to protect orbital assets.
(3)	3.1. Review QoS benchmarks emphasizing Quality of Experience (QoE) and real user data	1. Currently, Quality of Service (QoS) metrics in India focus on technical KPIs such as call drop rates and latency, which often do not reflect actual user experience. Many users in rural and semi-urban areas still report poor	1. To address these issues, crowd-sourced QoE measurement tools can be deployed to capture user experience data directly from devices. 2. Periodic QoS reports should be mandated based on real-user

		service despite operators meeting technical benchmarks. 2. Gathering large-scale, real-user data is difficult due to privacy concerns, varied device capabilities, and lack of standardized measurement tools. 3. Telecom operators may also resist stricter QoE benchmarks due to the costs of upgrading infrastructure and reconfiguring networks.	performance metrics, ensuring transparency and accuracy. 3. Operators could also be incentivized through performance-linked benefits to meet or exceed enhanced QoE benchmarks.
	3.2. Harmonize QoS standards with global benchmarks for indoor and outdoor services	1. There is significant variation in indoor coverage standards across different countries, which poses challenges when trying to align India's benchmarks with international best practices. 2. Indoor signal penetration remains a persistent challenge, especially in dense urban environments and high-rise buildings. 3. Furthermore, there is a lack of standardized QoS measurement methodologies that apply uniformly to both indoor and outdoor environments.	1. Adopt ITU and 3GPP-aligned QoS guidelines, but adapt them to India's unique geographic and socio-economic conditions. 2. Promote in-building solutions such as Distributed Antenna Systems (DAS), small cells, and signal boosters, especially in high-density urban zones. 3. Mandate uniform QoS testing protocols for both indoor and outdoor environments to ensure comparability of results.
	3.3. Redefine minimum acceptable signal strength and broadband speed	1. Current benchmarks for signal strength and broadband speed do not reflect modern application	1. Conduct nationwide technical studies to set updated, evidence-based thresholds for minimum

		demands, leading to poor QoS (quality of service) in many areas despite “coverage” being reported. 2. Variations in definitions across regions and service providers make enforcement inconsistent.	signal strength and broadband speed aligned with international best practices. 2. Make these thresholds legally enforceable under service-level agreements (SLAs) with penalties for persistent non-compliance.
	3.4. Roll out Digital Communication Readiness Index (DCRI) in a time-bound manner	1. Different states and departments may measure “readiness” differently , e.g., what counts as adequate connectivity in Delhi may not match rural Assam. 2. Many villages still have patchy telecom connectivity, making live performance monitoring difficult. 3. Surveys may be outdated or incomplete because of inaccessible terrain or low reporting capacity.	1. Set uniform definitions for parameters like coverage quality, download/upload speeds, latency, public Wi-Fi availability, and digital literacy rates. 2. Use TRAI/DoT as the nodal agency to maintain the standard. 3. Partner with Panchayats, CSCs (Common Service Centres), and post offices for regular data updates from rural areas. 4. Include number of trained digital facilitators, availability of e-governance services, and citizen awareness programs in the Index.

	3.5. Integrate telecom towers in NDMA disaster recovery protocols	1. Telecom towers are often not prioritized in disaster management plans, leading to delayed restoration of communication during crises. 2. Coordination gaps between telecom operators and disaster management authorities, leading to slow response times.	1. Formally integrate telecom tower infrastructure into NDMA's disaster recovery standard operating procedures. 2. Establish a dedicated coordination cell between NDMA, State Disaster Management Authorities (SDMAs), and telecom operators for rapid response.
	3.6. Promote transparency of telecom coverage and signal strength	1. There is currently no standardized, publicly accessible platform that provides real-time, location-specific telecom coverage and signal strength data across service providers. This lack of transparency makes it difficult for consumers to make informed choices and for authorities to identify coverage gaps, especially in rural or disaster-prone areas.	1. The Department of Telecommunications could create a unified, map-based portal displaying real-time signal strength and network coverage across all licensed operators, updated through automatic API feeds from telecom networks. This portal could also integrate feedback mechanisms for users to report poor service quality, allowing for quicker resolution and policy-level interventions.

	3.7. Encourage low-latency communications for industrial applications	1. In India, guaranteeing this level of performance demands substantial infrastructure investment in high-capacity fiber backhaul, edge data centers, and advanced 5G features like network slicing. This makes it difficult for operators to invest without a clear business case and predictable demand from industry. Spectrum dedicated to industrial use cases remains limited, and integration with legacy equipment in factories can cause delays and interoperability issues. 2. Additionally, small and medium enterprises (SMEs), which form a large part of Indian industry, may find the costs prohibitive without government support.	1. Prioritize dedicated spectrum in mid-band and mmWave ranges for industrial and private 5G/6G networks. 2. Provide policy incentives for edge computing infrastructure near industrial clusters to reduce latency and improve reliability. 3. Promote 5G network slicing pilots for sectors such as manufacturing, healthcare, and logistics, with partial government funding for trials. 4. Develop industry-specific interoperability standards to integrate low-latency solutions with older legacy systems. 5. Facilitate public–private partnerships in key industrial hubs (e.g., automobile manufacturing belts, pharma hubs) where costs and risks are shared. 6. Offer tax credits or capital subsidies to SMEs adopting low-latency communication solutions.
(4)	4.1. Ensure telecom/broadband services cost less than 2% of monthly GNI per capita	1. Broadband and telecom tariffs in certain regions still exceed the 2% affordability threshold, particularly for low-income households and rural users. 2. Lack of targeted subsidies or	1. Implement targeted tariff regulation or subsidy programs to bring effective costs within the 2% threshold. 2. Introduce transparent pricing policies requiring operators to

		low-cost packages for economically disadvantaged groups.	disclose all charges upfront.
	4.2. Incentivize small ISPs for last-mile broadband delivery	1. Small ISPs face high infrastructure setup costs and regulatory burdens, making last-mile connectivity financially unviable. 2. Limited access to affordable backhaul bandwidth and spectrum resources. 3. Larger operators often dominate urban areas, leaving rural markets underserved.	1. Provide tax breaks, low-interest loans, or infrastructure-sharing opportunities for small ISPs. 2. Establish government-supported backhaul networks accessible at low cost to smaller players. 3. Create a simplified licensing framework for small ISPs focusing on underserved regions.
	4.3. Facilitate convergence of NTN and terrestrial network for seamless access	1. Interoperability between satellite and terrestrial systems remains technically complex, with challenges in handover protocols, latency optimization, and bandwidth management. 2. Currently, the regulatory framework for NTN is fragmented between DoT, ISRO/IN-SPACe, and the Ministry of Information & Broadcasting, leading to licensing delays. 3. Additionally, hybrid NTN-terrestrial setups increase cybersecurity vulnerabilities, particularly if encryption and monitoring standards differ across	1. A unified regulatory framework that streamlines the licensing process for both NTN and terrestrial operators would reduce barriers to integration. 2. Promoting open, interoperable technical standards would help ensure seamless functionality between the two systems. 3. Finally, enhanced cybersecurity protocols and coordinated monitoring mechanisms would be essential to address the heightened security risks of hybrid networks.

		systems.	
	4.4. Enable convergence of services such as TV and e-Governance over telecom infrastructure	1. Delivering multiple services such as TV broadcasting and e-Governance applications over telecom infrastructure can face obstacles due to outdated legacy systems that are not optimized for multi-service delivery. 2. Quality of service may also suffer if content delivery is not adequately supported by existing bandwidth and infrastructure. 3. Additionally, coordination between government agencies and private telecom providers is often fragmented, creating bottlenecks in deployment.	1. upgrading telecom infrastructure to support the simultaneous delivery of multiple services without compromising quality. 2. Establishing service-level agreements (SLAs) and quality benchmarks would ensure consistent performance. 3. Creating formal inter-agency coordination platforms between public and private stakeholders could streamline operations and improve implementation efficiency.
	4.5. Promote infrastructure sharing among TSPs and utility sectors	1. While infrastructure sharing among Telecom Service Providers (TSPs) and utility sectors could significantly reduce costs and improve efficiency, it often encounters resistance due to commercial competition concerns. 2. There are also technical complexities in harmonizing different operators' systems, which could lead to incompatibility issues. 3. Moreover, improper sharing arrangements could result in	1. Mandating fair, regulated sharing frameworks would help ensure that commercial competition does not undermine collaborative benefits/ 2. Developing technical guidelines and binding SLAs would create clear expectations for operational standards. 3. Regular monitoring and enforcement of quality compliance would ensure that service standards are maintained despite shared infrastructure usage.

		degraded service quality if standards are not maintained.	
	4.6. Encourage common ducting in smart cities and linear infrastructure projects	1. Multiple service providers laying separate ducts increases cost, disrupts roads repeatedly, and delays project completion. 2. Limited awareness among contractors and municipal bodies about cost benefits of common ducting.	1. Develop national guidelines and standards for common ducting under smart city and linear infrastructure projects. 2. Conduct capacity-building workshops and awareness campaigns on the benefits and implementation methods of common ducting.

MISSION 2

Strategy No.	Provision	Issues Identified	Proposed Solutions
(1)	1.1. Fund R&D projects in emerging technologies, including AI, quantum security/communications, blockchain, AR/VR and 5G/6G.	1) The draft doesn't anchor funding calls to India's active national missions (Bharat 6G Vision; National Quantum Mission), risking duplication and thinly spread grants. 2) Outputs/KPIs (standards contributions, TRL jumps, patents) are unspecified. 3) No disclosure regime to track public ROI.	1. Rather than issuing broad, open-ended R&D calls, each funding round should be linked to ongoing national technology missions. For example, a call could be mapped directly to a specific Bharat 6G Vision workstream or a milestone in the National Quantum Mission roadmap. This ensures that funded projects are not working in isolation but are actively feeding into agreed national priorities, avoiding duplication and accelerating mission outcomes. 2. Every R&D award should clearly state the starting Technology Readiness Level (TRL) and commit to moving the project to a higher TRL for instance, from TRL 3 (experimental proof of concept) to TRL 5 (validated in relevant environment). In addition, recipients should deliver at least one tangible output such as a contribution to an international

			standards body or a patent application. To build transparency and competition, a yearly public scoreboard could showcase the TRL progression, standards contributions, and IP filings from all funded projects. 3. Where the project aligns with rural connectivity or affordability objectives, the Department of Telecommunications should co-finance trials using the Digital Bharat Nidhi (DBN) and its Telecom Technology Development Fund (TTDF) window. This integrated funding model would allow the same project to leverage both mission-based and rural-development R&D streams, while also enabling a single consolidated outcomes report across schemes making it easier to track and measure impact.
	1.2. Streamline the R&D ecosystem including funding, testing, certification, PoC facilitation, commercialization and market access.	1) Fragmented portals for grants, spectrum trials, and equipment approvals; innovators still hop between Saral Sanchar, WPC/ETA and lab bookings. 2) Uneven test-lab protocols; limited "PoC→procurement"	1. The Department of Telecommunications could establish a unified entry point that brings together all key processes for innovators in one place. This platform would handle grant applications, requests for experimental or technology-trial

		bridge.	licences, booking of lab and test-bed facilities, and even connections to OEM and PSU procurement opportunities. By linking it through APIs to existing systems like Saral Sanchar and the Wireless Planning and Coordination portal, applicants would avoid running through multiple disconnected processes. 2. To reduce costs and time for innovators, accredited telecom labs and 6G testbeds should adopt common test profiles and recognise each other's results. This means that once a device or solution passes testing in one recognised facility, the results would be valid in others, eliminating the need for repeat testing. 3. Any proof-of-concept that is successfully validated on a government-supported testbed should automatically qualify for small-lot pilot procurements by public sector undertakings and universal service providers. This would help promising solutions move more quickly from the lab to real-world deployment, while

			giving developers valuable early market feedback.
	1.3. Promote R&D in indigenous Telecom Chipset Development.	1) Design/fab gap: India's design ambition outpaces foundry access. 2) Shortage of VLSI design talent aligned to telecom PHY/RF. 3) Weak IP protection/valuation pathways for fabless startups.	1. Within the framework of the India Semiconductor Mission, a dedicated programme could fund tape-outs at partner foundries for validated chip designs. Priority lanes should be reserved for 5G and 6G RFICs (radio frequency integrated circuits) and baseband SoCs (system-on-chips). This would help accelerate indigenous design-to-fabrication cycles while ensuring that critical telecom hardware is developed domestically. 2. The government could sponsor long-term VLSI (Very Large-Scale Integration) academic chairs and practical chip-design programmes at IITs and NITs. These should be closely linked to Bharat 6G testbeds so that students and researchers gain hands-on exposure to live telecom innovation ecosystems. 3. To protect and commercialise innovation, a subsidised IP support system should be set up covering patent drafting, domestic

			and foreign filings, and portfolio management. This should be linked to the proposed IP-as-collateral financing pilot, enabling startups to borrow against their patent filings. Given the security needs outlined in the 6G roadmap and the National Quantum Mission's focus on quantum-safe systems, this framework should also ensure that chip-level designs integrate strong security from the outset.
	1.4. Collaborate with industry to establish a Section 8 company focused on promoting innovation.	1) Mandate/governance undefined → risk of overlap with TSDSI/B6GA/C-DoT. 2) Without revenue hooks, entity could be a pass-through grant box.	1. The proposed company should operate as India's execution arm for active participation in global telecom standards and for scaling technologies that are already at late Technology Readiness Levels (TRLs). It should avoid basic research, which can continue to be handled by universities and dedicated R&D centres. Instead, its role should be to take near-market solutions, integrate them into standards processes, and push them toward deployment. This would complement the work of the Bharat 6G Alliance and the Telecom Standards Development Society, India (TSDSI), which have recently signed an MoU to align India's standards activities.

			2. The organisation's board should have a majority of members from industry, supported by clear investment and conflict-of-interest policies published in the public domain. To ensure long-term sustainability, the company should work toward becoming financially self-sufficient within five years, generating revenue through activities such as intellectual property licensing and providing specialised testing and certification services to the telecom sector.
	1.5. Promote setting up of regulatory sandboxes.	1) Multiple sandbox hosts (DoT, MeitY, state missions) = inconsistent rules and timing. 2) Approval cycles still deter startups.	1. Create a single, standardised rulebook for all telecom sandboxes covering eligibility criteria, data-sharing norms, safety requirements, and time-bound service-level agreements of 30–60 days for approvals. The sandbox framework should operate in rolling cohorts so innovators can join without waiting for an annual call. 2. Any solution that successfully completes sandbox testing should automatically qualify for a technology-trial licence. These

			trial licences should come with pre-cleared spectrum bands and power limits to speed up deployment and reduce regulatory friction.
	1.6. Allow experimentation in Terahertz (THz) bands.	1) No pre-notified THz test segments; import/testing frictions. 2) Need to protect scientific services. 3) Policy should reflect India's emerging THz activity (IIT labs, 6G testbeds) and TRAI's stance.	1. Identify specific Terahertz spectrum slices that are non-interfering for both indoor and outdoor trials and publish them as "R&D windows." These should be available through a simplified Experimental Authorisation process, and in line with TRAI's recommendations, the permits should have a longer validity period to support extended testing cycles. 2. Create a green-channel clearance process for importing measurement instruments and related equipment when ordered by accredited labs or official testbeds, ensuring trials are not delayed by customs bottlenecks. 3. Work with ISRO and astronomy research bodies to develop shared-use protocols that prevent interference between telecom experiments and satellite or radio astronomy operations, ensuring responsible spectrum

			use.
	1.7. Introduce experimental authorization for telecommunication networks and services.	1) Historically slow/uncertain approvals; documentation varies. 2) Weak link from experiments to scaled pilots. 3) Startups face fee burden.	1. The recently introduced Experimental and Technology-Trial Licences should be institutionalised with clear, standardised application forms, defined eligibility tiers for academia, startups, and MSMEs, and publicly available service-level agreements for approval timelines. For low-risk indoor trials, a self-declaration mechanism through the Saral Sanchar portal could be enabled, allowing innovators to start work without lengthy approvals. 2. Where trial KPIs are met, applicants should be eligible for time-bound pilot deployments on live public networks, restricted to a defined user base and specific geographies. This would help validate technologies under real-world conditions before full-scale rollouts. 3. Startups and higher-education institutions should receive discounted licence charges for experimental and trial work to reduce financial barriers and encourage greater participation in

			early-stage telecom innovation.
	1.8. Identify assignment-exempt spectrum bands for M2M.	1) The policy doesn't list bands/technical masks; uncertainty hurts device planning. 2) Global harmonisation matters for ecosystem costs. 3) India is also moving on 6 GHz for Wi-Fi M2M plan should dovetail.	1. The Department should publish an updated package that clearly reaffirms licence-exempt use of the 865–868 MHz, 2.4 GHz, and 5.8 GHz bands, including defined limits for equivalent isotropically radiated power (EIRP), duty cycles, and certification requirements under Equipment Type Approval (ETA). This pack should also provide compatibility guidance for emerging technologies such as LoRa and 5G NR-RedCap to help manufacturers design for compliance from the outset. 2. As India moves to delicence the 5925–6425 MHz band, publish coexistence masks and indoor/outdoor operating rules that enable both M2M and Wi-Fi services to operate without harmful interference. This will ensure smooth adoption across devices and networks. 3. Introduce a simple, one-page conformity code for short-range devices (SRDs) and IoT radios that manufacturers can reference early in their design cycle. This

			code should be directly linked to WPC's Equipment Type Approval process to streamline compliance and reduce testing delays.
	1.9. Open greenfield bands for emerging technologies such as IoT, M2M, V2X, D2M etc.	1. No roadmap of which bands are being considered industry lacks clarity for device planning. 2. Risk of non-harmonised spectrum (e.g., ITU Region 3 norms). 3. No mechanism to trial band availability before full commercialization.	1. The Department should publish an updated package that clearly reaffirms licence-exempt use of the 865–868 MHz, 2.4 GHz, and 5.8 GHz bands, including defined limits for equivalent isotropically radiated power (EIRP), duty cycles, and certification requirements under Equipment Type Approval (ETA). This pack should also provide compatibility guidance for emerging technologies such as LoRa and 5G NR-RedCap to help manufacturers design for compliance from the outset. 2. As India moves to delicence the 5925–6425 MHz band, publish coexistence masks and indoor/outdoor operating rules that enable both M2M and Wi-Fi services to operate without harmful interference. This will ensure smooth adoption across devices and networks. 3. Introduce a simple, one-page

			conformity code for short-range devices (SRDs) and IoT radios that manufacturers can reference early in their design cycle. This code should be directly linked to WPC's Equipment Type Approval process to streamline compliance and reduce testing delays.
	1.10. Accelerate public R&D investment by improving use of Digital Bharat Nidhi (DBN).	1. No clarity on what portion of DBN is earmarked for innovation R&D. 2. Funds disbursed slowly due to bureaucratic process. 3. No public outcome tracking.	1. Mandate that at least 5% of the Digital Bharat Nidhi (DBN) corpus be earmarked specifically for telecom R&D, with the funds channelled through the Telecom Technology Development Fund (TTDF), which already has provisions to receive up to this amount. This would ensure a stable and predictable funding stream for high-priority innovation projects in the sector. 2. Implement a unified digital platform to handle the entire funding lifecycle, from application to approval, disbursement, and progress reporting. This would reduce administrative delays, improve transparency, and make access to funds more efficient for innovators. 3. Release a public report each

			year detailing how DBN funds earmarked for telecom R&D were allocated, the projects supported, and their measurable outcomes. This would create greater accountability and help track the programme's impact over time.
	1.11. Launch a Technology Readiness Level funding program.	1. TRL stages unspecified alignment with global standards missing. 2. Risk of projects stalling between prototype and deployment.	1. Organise telecom R&D funding into clearly defined Technology Readiness Level (TRL) categories: TRL 1–4 for basic research, TRL 5–7 for prototyping and system validation, and TRL 8–9 for pre-commercial pilots. These tiers should align with widely accepted NASA and EU definitions and be adopted as a standard reference across government schemes, as also suggested by NITI Aayog. This would make it easier to target resources appropriately and avoid mismatches between project maturity and funding type. 2. For projects that have moved beyond the research phase (TRL 5 and above), provide structured mentorship from industry experts and facilitate matchmaking with potential customers, investors, and partners. This will increase the likelihood of market adoption and scaling.

			3. Assign and publicly record TRL tags for all funded projects at the start and end of the funding cycle. This would give investors and policymakers a clear view of project maturity, while enabling transparent tracking of technological progress across funding programmes.
	1.12. Explore the establishment of a Sovereign Patent Fund with ... SEP pool.	1. No governance, FRAND safeguards, or feasibility/RIA requirement. 2. Risk of anti-competitive and trade tensions.	1. Before launching the initiative, commission a 12-month feasibility study combined with a Regulatory Impact Assessment (RIA) to evaluate potential economic benefits, implementation challenges, and global competitiveness. This would help ensure that the programme's design is evidence-based and financially sustainable. 2. Establish an independent governance framework with clear conflict-of-interest safeguards, transparent methods for asset and IP valuation, and adoption of FRAND (Fair, Reasonable, and Non-Discriminatory) licensing rules to encourage broad participation and fair use of essential technologies.

			3. Limit the initial scope to pilot projects that directly support domestic telecom manufacturing capabilities. This will allow proof-of-concept validation before scaling to broader applications. 4. Set clear key performance indicators, such as the number of products commercialised, patents filed, or standards contributions made and incorporate sunset clauses so that the initiative is reviewed and either renewed, restructured, or phased out based on performance. 5. Pair the initiative with grants for standards participation, ensuring that funded projects not only develop technology but also actively contribute to global standards, thereby enhancing India's strategic influence.
	1.13. Support the development of SEPs in emerging technologies by incentivizing domestic R&D.	1. No specifics on incentives (tax, grants). 2. No linkage to standards participation.	1. Introduce dedicated grants or tax credits for research and development projects that aim to generate Standard Essential Patents (SEPs) in priority telecom areas such as 5G, 6G, and IoT. This would help offset the high

			costs of SEP-oriented innovation and encourage Indian entities to invest in globally relevant technology development. 2. Cover participation expenses including membership fees, travel, and drafting support for Indian researchers, startups, and companies contributing to global Standards Development Organisations (SDOs). This ensures that promising technologies have a pathway from R&D into recognised global standards. 3. Require recipients of SEP-related incentives to commit to FRAND (Fair, Reasonable, and Non-Discriminatory) licensing terms and to ensure that the resulting SEPs are at least partially owned or controlled by Indian entities. This safeguards both global accessibility and national strategic interests.
	1.14. Explore the feasibility of accepting IPRs as collateral ...	1. No framework for valuation, registry, enforcement. 2. High lender risk-aversion absent guarantees.	1. Run a time-bound pilot programme in collaboration with SIDBI, the Reserve Bank of India, and selected public and private sector banks to test and refine intellectual property–backed

			lending models. This would create a controlled environment to identify operational challenges and market appetite before nationwide rollout. 2. Adopt uniform, government-recognised templates for IP valuation to ensure consistency and transparency across lending institutions. These templates should be developed in consultation with certified valuers and industry experts. 3. Provide partial loss guarantees for IP-backed loans to reduce the perceived lending risk for banks and encourage broader participation in the scheme. 4. Link the financing process to an IP charge registration system within the national IP registry, allowing lenders to verify ownership, record security interests, and monitor changes in real time. 5. Develop and deliver training programmes for credit officers on IP valuation, collateralisation processes, and recovery

			mechanisms. This will help address knowledge gaps and improve lending decisions.
	1.15. Augment C-DoT's resources through projectized proposals.	1. Unclear what "projectized" means. 2. Risk of duplication without coordination. 3. No commercialisation mandate.	1. Require all funded projects to clearly state their starting Technology Readiness Level (TRL), the TRL they aim to achieve by project completion, and a defined pathway to commercialisation. This ensures that R&D efforts remain focused on measurable progress and market relevance. 2. Give preference to initiatives that are jointly funded and executed with industry partners or academic institutions. Co-funding increases commitment from all parties, strengthens applied research outcomes, and accelerates the transition from prototypes to market-ready solutions. 3. Release a yearly public report summarising the funded project portfolio, their TRL advancements, patents filed, standards contributions, and commercial deployments. This will enhance transparency, showcase impact, and help refine

			future funding priorities.
(2)	2.1. Provide funding and mentorship from government/industry to telecom startups across growth stages, focusing on product development and market access.	1. The draft doesn't delineate support across different growth stages (seed, Series A, scaling). 2. Mentorship may not be telecom-domain specific. 3. No linkage to actual procurement or pilot deployment to validate market-readiness.	1. Establish a structured, multi-stage support model that caters to startups at different maturity levels. For example, a seed stage offering grants of up to ₹50 lakh, a growth stage with co-investment matching from private investors, and a scale stage focusing on market access facilitation. This could draw inspiration from C-DOT's Samarth programme, which provides smaller grants (around ₹5 lakh), lab access, and mentorship to early-stage innovators. 2. Curate a network of domain-specific mentors drawn from leading telecom R&D and incubation organisations, including senior technologists from C-DOT and the Software Technology Parks of India (STPI). Like in the Samarth model, these mentors can guide startups on both technology refinement and navigating regulatory or market-entry challenges. 3. Ensure that startups receiving scale-stage assistance have a direct pathway to test their

			solutions in real-world conditions. This could be done through partnerships with public sector undertakings or telecom service providers, enabling pilot deployments in live networks before broader commercial rollout.
	2.2. Introduce innovative financing models like Funds of Funds, Blended Finance etc., to expand funding opportunities for the pool of Telecom Startups in India.	1. The draft lacks reference to the existing Fund of Funds for Startups (FFS), which already catalyses funding at scale. 2. Blended finance concepts need structure to ensure leverage of private capital while maintaining accountability.	1. Leverage existing national Fund of Funds (FFS) programmes such as SIDBI's ₹10,000 crore corpus by earmarking a portion specifically for telecom-focused Alternative Investment Funds (AIFs). This could be implemented through a dedicated "telecom deep-tech window," ensuring that capital flows into high-potential areas like advanced networks, indigenous hardware, and critical telecom software systems. 2. Adopt a model where the government takes a first-loss position such as covering the first 20% of potential losses in telecom-focused venture funds. This approach, widely used in global blended finance best practices, reduces risk for private investors, encourages greater participation, and accelerates

			capital mobilisation into strategic telecom innovation. 3. Ensure that the investment committees of such funds include recognised telecom domain experts. Additionally, require all supported investments to demonstrate alignment with national telecom priorities, such as those outlined in the Bharat 6G Vision and the National Digital Communications Policy goals, to maximise sectoral impact.
	2.3. Organize annual events/competitions with government supported rewards and grants for winners, to encourage startups and innovators to develop cutting-edge telecom solutions.	1. Standalone contests may yield interest but lack follow-through, leading to "pitch tourism." 2. Winners might not translate ideas into pilots or products. 3. No expansion or strategic alignment with telecom events.	1. Design national-level telecom innovation contests where winners not only receive prize money ₹10 to ₹25 lakh in grants but also benefit from six months of structured mentorship and access to pilot opportunities with telecom operators or relevant government projects. This model could draw from Maharashtra's policies, which offer pilot procurement orders of up to ₹25 lakh for winning solutions, helping innovators move quickly from concept to market validation. 2. Launch annual hackathons focused on solving high-priority telecom challenges and link them

			to the India Mobile Congress (IMC), the country's largest digital and telecom industry event. Finalists could pitch directly to investors, industry leaders, and policymakers during IMC, while also showcasing their solutions on the event's exhibition floor for maximum visibility. 3. Create a grant programme targeted at early-stage telecom entrepreneurs under a model similar to WTFund, which provides ₹20 lakh or more in non-equity funding. By removing the need to give up ownership, such grants would encourage youth-led innovation in telecom and attract fresh talent to the sector.
(3)	3.1. Establish Tech Incubation Hubs with academia + industry.	Risk of duplication with existing STPI CoEs, MeitY-TIDE, and C-DOT Samarth incubators; small cohort sizes; scattered resources.	1. Establish a National "Hub Registry & Gap Map" by creating and maintaining a central database mapping all telecom-related incubation and innovation hubs in the country, along with a "gap map" that highlights underserved technology domains and geographic regions. This will help ensure resources are targeted where they are most needed and prevent clustering in already well-served areas.

			2. Require new incubation initiatives to sign Memoranda of Understanding (MoUs) with established hubs such as C-DOT's Samarth centres and STPI facilities to share laboratories, mentorship networks, and technical expertise. This will reduce duplication, lower operational costs, and accelerate access to infrastructure for startups. 3. Define performance benchmarks for all hubs, aiming for at least 60 startups incubated per year after the second year of operations. This will ensure that facilities operate at a scale that justifies public investment. 4. Release public, regularly updated dashboards tracking key metrics such as startup survival rates, patents filed, and proof-of-concept projects completed. This will enable stakeholders to monitor impact and hold programmes accountable for results.
	3.2. Facilitate research collaborations between	MoUs may not result in deployable products; unclear IP	1. Move to milestone-based cooperative agreements, where

	academia & private enterprises in AI, IoT, blockchain, etc.	ownership; short-term funding ending before pilot stage.	projects progress through clearly defined stages such as lab prototype development, field trials with telecom service providers, and achievement of Technology Readiness Level 6 or higher. This ensures funding is linked to tangible progress. 2. Predefine intellectual property terms in advance by using standardised agreement templates from collaborative frameworks such as the Indo-U.S. Science and Technology Forum (IUSSTF) or the U.S.-India Science and Technology Endowment Fund (USISTEF). This will reduce negotiation delays and provide clarity to all parties. 3. Require funded projects to deliver concrete contributions to recognised standards bodies, such as the Telecom Standards Development Society, India (TSDSI), 3GPP, or IEEE, ensuring alignment with global interoperability goals. 4. Link the release of the final funding tranche to clear evidence of commercialisation or pilot deployment, creating a strong

			incentive for projects to achieve market-ready outcomes.
	3.3. Encourage G2G, G2B, B2B collaboration in standards development & patenting.	Fragmented Indian participation in global SDOs; lack of travel/membership funding; weak mentoring for new contributors.	1. Establish a Standards Participation Grant to cover costs such as travel, membership fees, and expert mentoring for contributors to global telecom standards bodies. This programme should be anchored within the recently signed Bharat 6G Alliance–TSDSI MoU to ensure coordination and maximise India's influence in standards development. 2. Define clear national targets for standards engagement, such as the number of accepted contributions per release cycle, rapporteur or leadership roles held, and test specifications authored or owned by Indian participants. 3. Publish public leaderboards highlighting the performance of academia, SMEs, and other contributors in meeting these targets, creating healthy competition and visibility for top performers.
	3.4. Encourage international academic exchanges & global joint research.	Exchanges without pilots or IP; funds thinly spread; outputs limited to publications.	1. Prioritise international academic and industry exchanges that are directly linked to field pilots involving integration with

			telecom operators or service providers. This ensures that collaborations move beyond research into real-world deployment. 2. Utilise existing funding and collaboration platforms such as SPARC and IUSSTF, but update their evaluation criteria to place greater weight on commercialisation potential and joint intellectual property or standards contributions. 3. Leverage frameworks like the Initiative on Critical and Emerging Technology and other bilateral ICT cooperation tracks to establish joint testbeds in strategic areas such as 6G and telecom network security.
	3.5. Collaborate with DPIIT/CGPDTM to enhance telecom patent examiner capacity.	Backlogs, uneven quality in AI/CRI/SEP examination; high attrition.	1. Conduct quarterly upskilling programmes for patent examiners on emerging areas such as AI/CRI, 5G/6G technologies, and Standard Essential Patents (SEPs), with completion of these programmes linked to career progression and promotion criteria. 2. Organise international examiner exchange programmes with

			offices such as the Japan Patent Office, European Union Intellectual Property Office, and United States Patent and Trademark Office, focusing specifically on telecom-related cases to build global best-practice expertise. 3. Incorporate dedicated SEP-specific training modules into examiner development programmes to strengthen expertise in identifying, evaluating, and processing standard-essential telecom patents.
	3.6. Create Telecom Data Regulatory Sandbox for anonymized data use.	Risk of DPDP Act non-compliance; re-identification risk; limited SME participation.	1. Implement the framework in line with TRAI's 2024 sandbox recommendations and centralise all applications through a dedicated DoT Sandbox Portal, creating a single point of entry for innovators. 2. Require all sandbox projects to follow DPDP-compliant anonymisation practices, referencing standards such as BIS IS 17428 and the DSCI Privacy Framework, and to conduct a Data Protection Impact Assessment (DPIA) before launch. 3. Establish an independent

			privacy and ethics oversight board to review and monitor all sandbox activities, ensuring responsible use of telecom data. 4. Begin with pilot projects focused on clear public-benefit outcomes, such as the TRAI–RBI initiative on spam-call consent management, to build trust and demonstrate impact.
	3.7. Develop framework for accepting IPRs as collateral.	Banks lack valuation expertise; weak enforcement; high perceived risk.	1. Launch a pilot programme for IP-backed lending in partnership with SIDBI and selected public sector banks, using WIPO-aligned valuation methodologies and offering first-loss guarantees to reduce lending risk. 2. Establish a dedicated "IP Valuation Panel" to standardise valuation practices, and create a security-interest registry for intellectual property rights (IPRs) so lenders can record and track collateral in real time. 3. Integrate IP-backed lending with SIDBI's venture debt offerings to provide tailored financing solutions for IP-intensive MSMEs, enabling them to scale without diluting equity.

			4. Develop and deliver specialised training programmes for credit officers on IP finance, valuation, and recovery mechanisms to build institutional capacity and improve decision-making.
(4)	4.1. Advance development via global SDOs (e.g., 3GPP)	1) Participation costs (travel, membership, drafting time) deter MSMEs/academia; EU funds these explicitly, India mostly doesn't. 2) Fragmented voice across TSDSI/B6GA/industry risk of duplicated or late inputs to 3GPP/ITU. Recent MoUs help but need operational glue.	1. Create a Standards Participation Micro-Grant programme offering ₹2–5 lakh per meeting for MSMEs and academic institutions, tied to verifiable contributions in recognised standards bodies such as 3GPP, ETSI, and ITU (e.g., work items, liaison statements, and change requests). This could be modelled on StandICT.eu's travel and participation voucher scheme. *KPI:* number of funded delegates and number of accepted contributions per ₹10 lakh spent. 2. Establish a National 3GPP Tasking Calendar under the joint Bharat 6G Alliance (B6GA) and TSDSI framework that pre-assigns India "lead pen" responsibilities for priority work items in each release cycle, along with deadlines and designated owner laboratories. *KPI:* percentage of priority items with Indian rapporteurs or co-editors, and the number of Indian-

			led work items. 3. Fund SDO Training Bootcamps to equip participants with practical skills such as drafting change requests, managing liaisons, and adhering to IPR protocols. These could be supported through the Telecom Technology Development Fund (TTDF) or Digital Bharat Nidhi (DBN) and take inspiration from the EU SNS JU's standards translation training model. KPI: conversion rate from trained participants to actual standards submissions.
	4.2. Strengthen SDOs & fund participation (esp. MSMEs, startups, academia, public R&D)	1) No ring-fenced Indian fund like EU's SNS JU to bankroll standardisation outcomes; Indian projects often stop at papers/prototypes. 2) Grants rarely pay for the last mile (editorial time, test-vector packaging) needed for standards.	1. Launch a Standards Outcomes Top-Up incentive under the Telecom Technology Development Fund (TTDF), where publicly funded projects that successfully convert their results into accepted standards text such as a 3GPP change request (CR) being merged, receive a success bonus of ₹10–25 lakh. *KPI:* number of accepted specifications or CRs achieved per year. TTDF's existing governance framework can serve as the delivery mechanism. 2. Establish a National SDO

			Fellowship programme offering 1–2 year placements, including industry secondments, for PhD scholars and young engineers to work directly within key Standards Development Organisations (SDOs). This mirrors European models that fund researcher mobility and active participation in standardisation. *KPI:* number of fellows placed and number of liaison drafts or contributions they produce. 3. Publish transparent standards participation dashboards on a quarterly basis, detailing the number of Indian delegates per SDO, accepted contributions, and editorial or rapporteur roles. This can be modelled on EU SNS KPI scoreboards. *KPI:* dashboard goes live and demonstrates a quarter-on-quarter growth rate in participation and contributions.
	4.3. Explore CSR funding for standards work via recognised SDOs	1) CSR law limits spend to Schedule VII activities; standards development isn't named explicitly needs structuring via eligible buckets (incubators, R&D at public-funded institutions).	1. Issue a joint MCA/DoT clarification confirming that corporate social responsibility (CSR) funds can be channelled toward telecom standards activities under item (ix) of Schedule VII of the Companies

		2) Companies need clarity that CSR can legitimately fund pre-competitive standards work through approved entities.	Act. This would cover contributions to government-approved incubators or R&D programmes at publicly funded universities, IITs, CSIR, DBT, or DST institutions hosting standards cells. Provide a pre-vetted list of eligible host institutions to simplify participation. *KPI:* total CSR funds mobilised per year and the number of sponsored standardisation projects. 2. Create a CSR + Standards Matching Facility under the TSDSI and Bharat 6G Alliance (B6GA), where companies pledge CSR funds and the facility allocates them to vetted standards-related tasks such as testbed development, IPR landscaping studies, or drafting sprints. Publish model Memoranda of Understanding (MoUs) and impact reporting formats aligned with CSR compliance FAQs. KPI: number of CSR MoUs signed and the number of accepted SDO texts funded through this mechanism.
	4.4. Launch 6G Research & Innovation PhD Programme with Bharat 6G Alliance	1) India has set a 10% of global 6G patents ambition; converting PhD research into standards/SEPs needs structured funding, supervision, and global co-	1. Launch a 6G Research and Innovation PhD Programme in collaboration with the Bharat 6G Alliance (B6GA), targeting doctoral students working on

		advisors. 2) B6GA has active MoUs (TSDSI, EU/Finland/UK partners), but no nationally coordinated 6G PhD scheme yet.	advanced telecom technologies such as terahertz communications, AI-driven networks, and quantum-safe security. Provide stipends, research grants, and access to national testbeds to ensure high-quality outputs. KPI: number of enrolled PhD candidates, number of theses completed, and peer-reviewed publications or patents produced. 2. Pair each PhD fellow with both an academic supervisor and an industry co-mentor from leading telecom companies or R&D organisations. This dual-mentorship model will ensure research is both technically rigorous and market-relevant. KPI: proportion of projects with industry co-supervision and number of industry-supported trials or pilots conducted. 3. Link completion of the programme to tangible contributions in areas such as standardisation, intellectual property creation, or commercial prototypes, ensuring research outcomes feed directly into India's 6G development roadmap. KPI:

			number of standardisation contributions, SEPs, or deployable prototypes originating from the programme.

MISSION 3

Strategy No.	Provision	Issues Identified	Proposed Solutions
(1)	1.1. Develop industry-aligned courses on telecom engineering, electronics design, AI, cybersecurity, 5G/6G, IoT, quantum communication	1. Many institutions still teach outdated theory-heavy curricula, leaving graduates without the practical skills the telecom manufacturing sector needs. 2. Shortage of qualified faculty in emerging technologies like 6G and quantum communication; existing "train-the-trainer" funding may be overstretched. 3. Shared lab models risk concentrating in urban hubs, leaving tier-3 institutions behind. 4. Awareness campaigns for such programs often lack measurable targets.	1. Partner with industry leaders through enforceable MoUs tracked via blockchain, ensuring live projects and internships are part of the syllabus. 2. Establish "train-the-trainer" programs with a ring-fenced DBN skilling budget, incentivising faculty to obtain global certifications. 3. Set up regional shared labs under PPP models with mandatory 30% capacity for tier-3 institutions, funded under PLI/DBN. 4. Launch national awareness drives tied to KPIs (e.g., 20% yearly enrolment growth) with scholarships for underrepresented groups.
	1.2. Implement and institutionalize apprenticeship and internship programs in telecom sector in line with PM's Internship Scheme	1. SMEs often lack facilities and trained mentors to host apprentices. 2. Academic calendars don't align well with industry project cycles; virtual components risk excluding	1. Offer SME-specific quotas under PLI extensions with grants to set up apprentice facilities. 2. Use flexible, modular timelines but require minimum broadband standards for any virtual element.

		rural areas due to poor internet. 3. Lack of consistent evaluation metrics; certification delays are common. 4. Women and rural youth participation limited by relocation, safety, and affordability issues.	3. Roll out a national digital certification portal with joint industry–academia governance. 4. Ensure host organisations comply with safety audits and diversity protocols, and provide stipends, travel allowances, and gender-safe housing.
	1.3. Sponsor partnership programs between industry and academia (including DoT training institutes) to bridge skill gaps in high tech telecom technology areas	1. Current funding tends to favour urban partners; rural allocations may stretch DBN's core mandate for connectivity. 2. Rigid IP agreements discourage open-source models. 3. Approval backlogs in DoT processes delay partnerships. 4. MNCs may choose global R&D hubs over Indian academia.	1. Ring-fence 10% of DBN funds for skilling partnerships in rural/underserved areas. 2. Use flexible IP templates with arbitration clauses to balance open and proprietary outputs. 3. Integrate approvals into the Saral Sanchar portal with fast-track workflows. 4. Tie MNC benefits to export-linked incentives or preferential market access.
	1.4. Strengthen the Telecom Sectoral Skill Council (TSSC) for skilling activities at regional level in collaboration with state governments and other stakeholders	1. TSSC presence is uneven; poorer states risk being left behind. 2. Frequent updates to course content can be resource-intensive; large companies may dominate input. 3. State-level skill initiatives can overlap with TSSC's work.	1. Offer central matching grants to low-income states to expand coverage. 2. Ensure diverse industry representation in content-update panels. 3. Integrate TSSC into a unified national skill portal to avoid duplication.

		4. Tracking employment outcomes raises privacy issues.	4. Apply GDPR-style privacy safeguards to alumni tracking while tying funding to verified placements.
	1.5. Leverage 5G/6G use case labs for providing trainings in advance mobile technologies	1. High capex/opex; past PLI disbursal delays risk slowing deployment. 2. Dependence on foreign trainers erodes self-reliance goals. 3. Uniform national curricula may overlook regional sector needs. 4. Unlimited MSME access could overload lab capacity.	1. Enforce strict timelines on PLI/DBN fund releases for lab setups. 2. Prioritise domestic trainers with international certifications. 3. Layer region-specific modules on top of a national framework. 4. Implement lab booking quotas for MSMEs to manage usage.
	1.6. Engage DoT field units in promoting telecom skilling initiatives	1. Adding skilling duties without recruitment risks overburdening staff. 2. Local campaign branding varies and may dilute impact. 3. Poor connectivity in rural field units hampers coordination. 4. KPI frameworks sometimes value enrolment numbers over real outcomes.	1. Allocate dedicated skilling officers within DoT field units. 2. Provide national branding kits to keep messaging consistent. 3. Fund connectivity upgrades for rural DoT offices. 4. Focus KPIs on job placements and skill application rates, not just enrolment.
(2)	2.1. Provide targeted CAPEX/OPEX support to boost domestic telecom manufacturing	1. PLI expansion risks spreading funds too thin; processing delays persist. 2. SMEs without adequate tech infra are left behind. 3. Complex SME tier structures	1. Cap component allocations at 20% of the PLI corpus to protect funds. 2. Provide SMEs with technical onboarding support. 3. Simplify eligibility tiers with

		add red tape. 4. Overly intrusive audits deter applications.	automatic qualification triggers. 4. Shift to AI-enabled, low-intrusion audits.
	2.2.Incentivize Telecom and networking Software Development	1. Overlaps with NSDC training; waste of resources likely. 2. Patent offices overburdened, causing delays. 3. Export subsidies could violate WTO norms. 4. VC funding is concentrated in urban hubs.	1. Form joint oversight committees with NSDC to avoid duplication. 2. Expand patent office staffing using NTP-2025 funds. 3. Redesign export incentives as R&D-linked grants for WTO compliance. 4. Reserve 40% of DBN-backed VC funds for rural startups.
	2.3. Incentivize telecom operators to use indigenously designed and manufactured equipment	1. Local quality perception is poor; rebates may be insufficient. 2. Testing delays slow adoption. 3. Showcase pilots can be biased. 4. Warranty mandates are risky for weak supply chains.	1. Tie rebates to verifiable quality improvements. 2. Fast-track TEC testing processes. 3. Use neutral third-party auditors for pilot evaluations. 4. Phase in warranty requirements alongside supply-chain support.
	2.4. Promote "Made in India" telecom products globally through brand building activities, with a focus on innovation and quality assurance	1. Weak data on priority export markets. 2. FTAs take years to close. 3. Over incentivising risks oversupply. 4. SMEs may not access EXIM funding.	1. Base campaigns on deep market research. 2. Focus on quick-win trade agreements in parallel with long-term FTAs. 3. Cap incentives to match forecast demand.

			4. Assign SME quotas in EXIM credit schemes.
	2.5. Encourage investments in partner countries leveraging Line of Credit	1. Geopolitical risk analysis often incomplete. 2. Awareness of LoC schemes is low. 3. Insurance costs are a barrier. 4. India-centric tech pitches may ignore partner country needs.	1. Deploy AI risk-monitoring tools. 2. Pair LoC promotions with targeted trade fairs. 3. Subsidise LoC investment insurance. 4. Customise solutions for local partner contexts.
	2.6. Enhance export competitiveness of Indian telecom products by streamlining regulations	1. Telecom exporters face multiple approvals from different agencies, often with redundant documentation. 2. Indian products may not fully match international telecom standards (e.g., ITU, ISO, IEC), limiting market access.	1. Create a single-window clearance system for telecom exports, integrating all approvals and certifications. 2. Align domestic technical regulations with global benchmarks, and provide exporters with pre-certification support for target markets.
	2.7. Simplify and rationalize telecom equipment certification processes	1. Tight timelines risk quality checks. 2. Centralisation can cause bottlenecks. 3. Fee waivers may be misused. 4. Weak integration with evolving global standards.	1. Keep time limits but embed mandatory quality review steps. 2. Set up regional/distributed certification nodes. 3. Restrict waivers to vetted applicants. 4. Align standards annually with ITU/IEC norms.
	2.8. Strengthen ranking framework for labs	1. Audits are costly in money and	1. Outsource audits to certified

	accredited by TEC	manpower. 2. Expansion without controls could dilute standards. 3. Upgrade incentives can be gamed. 4. Current rankings have little global recognition.	external firms. 2. Set basic entry criteria before ranking labs. 3. Link upgrades to measurable gains in performance. 4. Negotiate mutual recognition agreements with global bodies.
(3)	3.1. Introduce support mechanisms for design-led manufacturing and enhancing domestic value addition	1. PLI grants alone don't cover high-risk design R&D. 2. Domestic IP policies overlook joint global development. 3. Design tool training is not continuous. 4. Value-add audits lack consistency.	1. Add venture and matching funds for design innovators. 2. Incentivise co-developed IP with global partners. 3. Bake ongoing tool training into TSSC programs. 4. Use standardised audit metrics for value-add verification.
	3.2. Make available spectrum for Captive Non-Public Network (CNPNs) and private 5G for industrial use cases	1. Possible reduction in public spectrum availability. 2. Subsidies can distort competition. 3. Interference controls may be weak. 4. Approval backlogs.	1. Introduce spectrum-sharing models. 2. Limit subsidies to key strategic sectors. 3. Mandate interference-mitigation tech. 4. Automate approval pipelines with strict SLAs.
	3.3. Incentivize strengthening of testing and certification lab ecosystem	1. DBN allocations too small to meet needs. 2. OPEX often ignored in planning.	1. Combine private investment with DBN for funding. 2. Include OPEX support in incentives. 3. Avoid duplication via

		3. Risks of TSSC role duplication. 4. Labs concentrated in certain regions.	coordinated action plans. 4. Distribute labs based on regional demand mapping.
	3.4. Facilitate Testing and Certification of Indian telecom products for foreign markets	1. MRAs progress slowly due to diplomatic processes. 2. Subsidies don't meet all costs. 3. Pre-testing adds delays. 4. Workshops alone don't ensure compliance.	1. Prioritise MRAs with top export targets. 2. Adjust subsidies based on firm size/need. 3. Link pre-testing to domestic lab checks. 4. Provide ongoing export compliance advisory services.
	3.5. Explore Mutual Recognition Agreements for conformity assessment and testing	1. Negotiations drag on. 2. Misalignment with evolving standards. 3. No dedicated oversight after signing. 4. Current scope too narrow.	1. Set fixed deadlines for negotiations. 2. Conduct annual standard harmonisation reviews. 3. Fund a dedicated post-MRA monitoring team. 4. Expand agreements to include more product categories.
	3.6. Harmonize Indian testing requirements with the global requirements	1. Frequent global standard changes disrupt industry. 2. Resource constraints for timely updates. 3. Industry reluctance to adopt new tests. 4. Consultation bias towards certain players.	1. Offer transition periods for new requirements. 2. Allocate budget specifically for updates. 3. Provide incentives for early compliance. 4. Involve a broad stakeholder mix in consultations.

MISSION 4

Strategy No.	Provision	Issues Identified	Proposed Solutions
(1)	1.1. Incentivize early development of security measures for future threats	1. New security technologies need huge investment with unclear returns 2. Small telecom companies cannot afford to invest in untested security solutions 3. Companies resist changing their current working security systems	1. Government should provide funding and tax benefits for security research 2. Create safe testing areas where companies can try new security without full regulations 3. Offer grants specifically for quantum-safe and AI security development
	1.2. Roll-out of quantum secured products	1. Quantum security technology is still new and very expensive 2. No global standards exist for quantum-safe methods 3. Very difficult to integrate with existing telecom networks	1. Start with government and critical networks first, then expand gradually 2. Partner with international research organizations to develop standards 3. Set up special labs to test and certify quantum security products
	1.3. Develop telecom infrastructure that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and telecom network	1. Building dual security systems is technically very complex and costly. 2. Old systems cannot support new quantum security without major upgrades. 3. Not enough experts who understand both old and new	1. Create frameworks that allow easy switching between different security methods 2. Start training programs for cybersecurity professionals on quantum technologies 3. Develop certification programs for hybrid security systems

		security methods.	
	1.4. Support cryptographic agility and a quantum-safe upgrade path for telecommunications network	1. Changing network security requires major changes to current infrastructure 2. During transition periods, networks may become more vulnerable 3. Different telecom companies may use different methods, causing compatibility issues	1. Set national standards for how to implement flexible security systems 2. Create a central coordination system to manage security transitions across all operators 3. Make compatibility testing mandatory for all new security implementations
	1.5. Prepare for quantum communications and Quantum-Safe Cryptography (QSC) to secure telecom data	1. Compatibility with Existing Telecom Infrastructure 2. International Interoperability & Cross-Border Data 3. Cybersecurity Liability	1. Phased implementation with transitional provisions (for example, full compliance in 5-10 years). Offer tax breaks or subsidies to telecom providers who adopt QSC. 2. Require interoperability testing prior to enforcement deadlines. 3. Align the national statute with the NIST Post-Quantum Cryptography Standards and the ETSI QSC guidelines. Incorporate mutual recognition agreements (MRAs) for QSC compliance with key partner countries. 4. Clearly assign liability in statute (for example, manufacturer for defects, telecom for improper deployment). Require cyber insurance for QSC-

			certified systems.
	1.6. Promote end-point security for telecom network device by deployment of indigenous endpoint detection & response solution	1. Developing local security products needs heavy investment and may lag behind global products 2. Telecom operators prefer proven foreign solutions over new domestic ones. 3. Doubts about whether local solutions work as well as international ones	1. Give financial incentives and priority in government purchases for local security products 2. Create partnerships between government and private companies to develop local solutions 3. Set up testing systems to prove that local solutions work effectively
	1.7. Promote 100% IPv6 adoption for proliferation of internet-connected devices	1. Many existing systems still use old IPv4 technology and cannot easily switch 2. Companies need technical skills and money to upgrade their network infrastructure 3. Some internet devices have limited support for new IPv6 technology	1. Make IPv6 support mandatory for all new telecom equipment and services 2. Provide training and certification programs for network engineers 3. Create incentive programs and set clear timelines for IPv6 migration
	1.8. Enforce cybersecurity frameworks based on adoption of AI/ML technologies such as AI Incident Reporting used in telecom services and network	1. AI security systems need huge amounts of data for training 2. Concerns about AI making biased or unreliable security decisions 3. Integrating AI with existing security systems is complex and expensive	1. Create secure data-sharing systems for AI training while protecting privacy 2. Develop standards for AI security systems that require transparency 3. Set up certification programs for AI-based security solutions
	1.9. Develop AI-specific telecom security standards to address risks from	1. AI security threats change very quickly, faster than traditional security can handle	1. Set up specialized AI security research centers with universities 2. Create rapid response teams

	adversarial AI, model drift, and automated threat propagation	2. Limited expertise in AI-specific security threats within telecom companies 3. Current security standards do not cover AI-related vulnerabilities	specifically for AI security threats 3. Design security standards that can be updated quickly as AI threats evolve
	1.10. Define policy and regulatory framework for blocking rogue IPs/URLs/Applications and its implementation in TSP/ISP network	1. Overbroad definitions like Vague terms (“harmful”, “rogue”) risk misuse or over-blocking. 2. Cross-border hosting-Many rogue servers are offshore; jurisdictional enforcement issues. 3. Cost burden on ISPs Smaller ISPs may lack resources for real-time blocking systems.	1. Define terms clearly and use internationally recognised categories (ITU, IETF). 2. Enable cooperation through MLATs, join CERT coordination networks, and use ISP-level geoblocking for non-cooperating states. 3. Offer subsidies, tax breaks, or shared government-managed blocking infrastructure.
	1.11. Strengthen national capability in telecom-specific cybersecurity threat intelligence, response, and recovery	1. Ambiguous scope and definitions.Operators, vendors, and regulators may interpret terms such as "cybersecurity threat intelligence" or "telecom-specific" differently. 2. The confidentiality of shared threat dataOperators may be hesitant to share logs/IOCs for fear of regulatory repercussions, competitive harm, or legal liability.	1. Define terms precisely in the statute (for example, use ITU, NIST, or GSMA FS-series definitions) and specify what constitutes telecom network elements (core, access, signalling, OSS/BSS). 2. Include safe harbour provisions for good faith reporting; require non-disclosure protection for sensitive operational data; and encrypt all shared intelligence.

		3. Conflict with privacy laws. Collection and sharing of telecom traffic data for threat analysis may conflict with personal data protection laws. 4. jurisdictional gaps in cross-border threats. Many telecom cyber threats originate on foreign networks or infrastructure.	3. Limit collection to metadata required for security; anonymise where possible; and require judicial or regulator-approved exceptions for DPI. 4. Include provisions for international CERT cooperation, MLATs, and cross-border intelligence sharing agreements.
	1.12. Finalize the blueprint of National Telecom SafeNet with close collaboration with MHA, TSPs and LEAs and expedite sanction of project and its funding	1. Coordinating between multiple government agencies is slow and complex 2. Different agencies may have conflicting goals and jurisdictions 3. Getting enough budget for such a large national project is challenging	1. Create a dedicated National Telecom SafeNet Authority with clear responsibilities 2. Set up standardized procedures for agencies to work together 3. Implement phased funding with clear milestones and measurable results
	1.13. Establish a mechanism to oversee and verify connected telecommunication equipment as trusted products with valid Certificates of Conformity	1. Equipment certification process is lengthy and complicated 2. Limited number of accredited testing labs for comprehensive verification 3. Keeping updated lists of trusted equipment requires continuous monitoring	1. Simplify certification through digital automation and online processes 2. Set up more accredited testing laboratories across the country 3. Create a dynamic database of trusted vendors with regular audits
(2)	2.1. Develop human resource and infrastructure for implementation of	1. Severe shortage of qualified cybersecurity professionals in telecom sector	1. Set up specialized cybersecurity training institutes in partnership with industry

	Telecom Cyber Security Rules, 2024 and Critical Telecommunications Infrastructure Rules, 2024	2. Current infrastructure is not adequate for comprehensive cybersecurity monitoring 3. Training programs cannot keep up with rapidly changing cyber threats	2. Create scholarship and fellowship programs for cybersecurity education 3. Develop shared infrastructure models to reduce costs for individual operators
	2.2. Evolve a comprehensive Cybersecurity Skills Framework, in consultation with stakeholders, to define critical competencies for roles such as Security Administrators, Security Analysts, and Penetration Testers	1. Current cybersecurity training programs do not match industry requirements 2. No standard way to evaluate cybersecurity skills across different organizations 3. Cyber threats evolve so fast that skill requirements keep changing	1. Create a National Cybersecurity Skills Council with representatives from industry, academia, and government 2. Develop standardized certification programs for different cybersecurity roles 3. Require ongoing professional development for cybersecurity professionals
	2.3. Strengthen Telecom CSIRT for cyber security incident reporting & mitigation including CTI monitoring	1. Current incident response teams lack the scale to handle modern cyber threats 2. Delays in incident reporting and response due to poor coordination 3. Limited sharing of cyber threat information between different organizations	1. Set up regional incident response centers for faster response times 2. Create automated systems for real-time incident reporting and threat sharing 3. Develop standardized procedures for sharing cyber threat information across sectors
	2.4. Examine and promote implementation of minimum cybersecurity controls for all telecom operators, based on global standards	1. Smaller telecom operators lack resources for comprehensive cybersecurity measures 2. Different operators may interpret and implement security standards differently	1. Create tiered cybersecurity requirements based on operator size and risk level 2. Provide technical assistance and shared resources for smaller operators

		3. Weak systems for monitoring and enforcing compliance	3. Set up automated compliance monitoring systems with regular audits
	2.5. Host annual events/competitions for robust testing of telecommunication network and create awareness for best practices	1. Industry players may not participate enough in cybersecurity competitions 2. Competitive formats may not accurately simulate real-world security challenges 3. Knowledge gained from events may not reach the broader industry effectively	1. Offer significant incentives and recognition for participating in cybersecurity competitions 2. Create realistic testing environments that mirror actual telecom networks 3. Establish platforms for sharing best practices identified through competitions
(3)	3.1. Enhance monitoring mechanisms to ensure that only standardized, security-certified, and trusted telecom equipment are used in critical infrastructure	1. Monitoring equipment across vast telecom networks is technically challenging and expensive 2. Equipment may be modified or compromised after initial certification 3. Limited visibility into equipment used by smaller operators in remote areas	1. Use blockchain-based tracking systems for tamper-proof equipment monitoring 2. Develop automated scanning tools to verify deployed equipment 3. Make mandatory reporting requirements for all critical infrastructure equipment
	3.2. Develop AI and other technology-based tools for detection and prevention of cyber frauds using the telecom ecosystem	1. AI fraud detection systems need extensive training data which may not be available 2. False alarms in fraud detection can disrupt legitimate communications 3. Integrating with existing fraud prevention systems is complex	1. Create data sharing frameworks for fraud detection while protecting user privacy 2. Build testing environments for validating AI fraud detection systems 3. Develop hybrid approaches combining AI with human expertise

	3.3. Define a framework for telecom security audit & empanelment of agencies thereof	1. Limited qualified agencies capable of conducting comprehensive telecom security audits 2. Audit standards and methods may not be consistent across different agencies 3. Cost of comprehensive security audits may be too high for smaller operators	1. Set minimum qualification requirements and certification for audit agencies 2. Create standardized audit methods and reporting formats 3. Develop cost-sharing mechanisms or subsidized audit programs for smaller operators
	3.4. Establish the SATCOM Monitoring Facility (SMF) to monitor Indian and foreign satellites and improve mitigation of satellite carrier interference	1. Setting up satellite monitoring requires significant technical infrastructure and expertise 2. Monitoring foreign satellites may have international legal implications 3. Interference resolution requires coordination with multiple international parties	1. Establish partnerships with international space agencies for satellite monitoring 2. Develop automated systems for detecting and resolving interference 3. Create legal frameworks for addressing satellite interference through diplomatic channels
	3.5. Increase monitoring of radio frequency and establish Wireless Monitoring Stations along the border areas to reduce cross-border spillage	1. Border areas often have difficult terrain and limited infrastructure 2. Cross-border spectrum coordination requires diplomatic engagement with neighboring countries 3. Maintaining monitoring equipment in remote border areas is logistically challenging	1. Use existing border security infrastructure for spectrum monitoring 2. Develop mobile and portable monitoring solutions for difficult terrain 3. Establish bilateral agreements with neighboring countries for spectrum coordination
	3.6. Put in place adequate and effective regulatory framework to prevent	1. IMEI cloning and manipulation are sophisticated crimes that are difficult to detect	1. Implement blockchain-based IMEI tracking systems for tamper-proof identification

	misuse of Telecom Identifiers (including IMEIs)	2. International coordination is needed to track devices across borders 3. Current enforcement mechanisms are inadequate to deter identifier misuse	2. Establish international cooperation frameworks for cross-border device tracking 3. Create severe penalties and strong enforcement mechanisms for identifier misuse
	3.7. Put in place adequate and effective regulatory framework and systems to detect and prevent unsolicited commercial communication (UCC)/ spam	1. Spam detection systems may block legitimate messages by mistake 2. Spammers continuously develop new techniques to bypass detection systems 3. Cross-border spam requires international coordination for effective prevention	1. Use AI-powered spam detection with continuous learning capabilities 2. Create real-time sharing of spam blacklists between operators 3. Establish international cooperation frameworks for combating cross-border spam
	3.8. Conduct analysis of telecom and networking equipment deployed in TSP network to demarcate and segregate equipment from non-trusted sources	1. Analysing equipment across vast telecom networks requires significant resources 2. Non-trusted equipment may already be deeply integrated into network operations 3. Segregating equipment may disrupt ongoing services and require large investment	1. Develop automated equipment analysis tools using AI and machine learning 2. Create phased segregation plans to minimize service disruption 3. Provide financial assistance for replacing equipment from trusted sources
	3.9. To continuously engage with relevant stakeholders like TSPs/ISPs, law enforcement agencies, financial sector entities to prevent misuse of telecom resources for cybercrime	1. Operators, vendors, and regulators may interpret terms such as "cybersecurity threat intelligence" or "telecom-specific" differently. 2. The confidentiality of shared threat dataOperators may be hesitant to share logs/IOCs for	1. Define terms precisely in the statute (for example, use ITU, NIST, or GSMA FS-series definitions) and specify what constitutes telecom network elements (core, access, signalling, OSS/BSS). 2. Include safe harbour provisions

		fear of regulatory repercussions, competitive harm, or legal liability. 3. Collection and sharing of telecom traffic data for threat analysis may conflict with personal data protection laws. 4. Many telecom cyber threats originate on foreign networks or infrastructure.	for good faith reporting; require non-disclosure protection for sensitive operational data; and encrypt all shared intelligence. 3. Limit collection to metadata required for security; anonymise where possible; and require judicial or regulator-approved exceptions for DPI. 4. Include provisions for international CERT cooperation, MLATs, and cross-border intelligence sharing agreements.
	3.10. To introduce Mobile Number validation Service for providing a secure telecom space to other services sector entities like banking, insurance, social media, e-governance etc. for prevention of misuse of telecom resources for cyber frauds	1. Creating a centralized validation service requires significant infrastructure and security 2. Different sectors may have varying validation requirements and standards 3. Privacy concerns about centralized storage and access to mobile number data	1. Implement privacy-by-design principles in the validation service architecture 2. Create sector-specific validation systems with appropriate security controls 3. Establish clear data governance and access control frameworks
	3.11. Citizen empowerment and engagement through portal, app and tools offered through 'One Stop Solution' to prevent misuse of telecom resources for cybercrime and financial	1. Citizens may lack awareness about available tools for fraud prevention 2. Cybercrime complexity makes it difficult for citizens to understand and report issues 3. Digital literacy levels vary	1. Implement comprehensive awareness campaigns through multiple channels 2. Develop user-friendly interfaces with multilingual support and voice interactions 3. Create educational programs

	frauds	significantly among different user groups	on cybersecurity awareness for different groups
	3.12. Promote community outreach and public awareness campaigns on safety and trustworthiness of telecom network and services	1. Public awareness campaigns may not effectively reach all groups, especially rural areas 2. Technical information about telecom security is difficult for general public to understand 3. Misinformation about telecom technology may persist despite awareness efforts	1. Develop targeted campaigns for different demographic groups using appropriate channels 2. Create simple, easy-to-understand educational materials about telecom security 3. Engage local community leaders and influencers in awareness campaigns
	3.13. Engage with global partners to develop shared strategies, best practices, and cross-border frameworks to tackle international spam, fraud and phishing, reinforcing India's role as a trusted digital nation	1. International cooperation requires diplomatic engagement and may be slow to implement 2. Different countries have varying legal frameworks and enforcement capabilities 3. Information sharing across borders is limited by privacy and sovereignty concerns	1. Establish bilateral and multilateral cybersecurity cooperation agreement 2. Create standardized information sharing protocols that respect national sovereignty 3. Participate actively in international cybersecurity forums and organizations
	3.14. Formulate mandatory business continuity and disaster recovery frameworks for telecom network to ensure resilience during physical or cyber disruptions	1. Developing comprehensive business continuity plans requires significant investment and expertise 2. Testing and validation of disaster recovery plans may disrupt ongoing operations 3. Coordination between multiple operators during disasters is challenging	1. Provide templates and guidelines for business continuity planning 2. Create shared disaster recovery infrastructure to reduce individual operator costs 3. Establish regular drill exercises and testing requirements for disaster recovery plans
	3.15. Ensure secure integration of emerging	1. Emerging technologies may not have mature security	1. Establish security-by-design requirements for all emerging

	technologies (quantum, edge AI, IoT, MEC, NTN) into the trusted network framework	standards and frameworks 2. Integration of new technologies with existing security infrastructure can create vulnerabilities 3. Rapid pace of technological change may outpace security standard development	technology implementations 2. Create rapid security assessment and certification processes for new technologies 3. Develop adaptive security frameworks that can evolve with technological changes
	3.16. Establish Centre for Excellence (COE) for promoting and enhancing use of Artificial Intelligence in Telecom Cyber Security.	1. Establishing a center requires significant initial investment and ongoing funding 2. Attracting and retaining top AI and cybersecurity talent is challenging 3. Industry engagement may be limited without clear value propositions	1. Develop public-private partnership models for funding and operation 2. Create attractive career progression and research opportunities to attract talent 3. Establish clear industry engagement frameworks with measurable benefits

MISSION 5

Strategy No.	Provision	Issues Identified	Proposed Solutions
(1)	1.1. Implement in-building solutions and encourage adoption of rating of buildings w.r.t telecommunication connectivity by town planner/municipal bodies (Tier 1 and Tier 2);	1. There is no established benchmark for telecom ratings, making it difficult to compare buildings based on telecom performance. 2. There may be no motivation for builders to adopt in-building telecom solutions since there may not be instant market demand. 3. Existing buildings may not be able to adopt these solutions, especially in congested cities.	1. A uniform rating system should be introduced throughout the country in collaboration with government agencies and industry bodies. 2. The policy may suggest potential benefits to builders, including options like ranking cities based on the uniform rating system (proposed earlier) and public recognition schemes. 3. The policy can propose government aid to remodel buildings to fit the norms of the policy.
	1.2. Study and devise special packages for minimum usage as per ICT Development Index 2024 for ensuring affordability for lower economic strata of the society;	1. At the ground level, there is very limited real-time data that can give an accurate representation on the exact needs of the lower economic strata. This will lead to a disconnect between the National Index and Local Implementation. 2. The use of a one-size-fits-all kind of subsidiary models that will ensure affordability may not apply to people who need them due to	1. The policy can recommend targeted surveys at the grass root level to identify the issues faced. 2. The policy can recommend the integration of such benefit schemes with systems like Aadhar-linking, or other welfare schemes like Direct Benefit Transfer (DBT). 3. The policy can recommend a reduced Universal Service

		practical issues like lack of documentation. 3. There is a possibility of resistance from Telecom Service Providers in the absence of any benefit to them.	Obligation Fund (USOF) contribution in exchange for providing subsidized packages to the rural area, considering that the whole purpose of the USOF is to extend telecom services to rural areas.
	1.3. Work in collaboration with MHA to establish a resilient Public Protection and Disaster Relief (PPDR) network;	1. There is no dedicated and uniform pan-India spectrum explicitly set aside for PPDR needs that may arise, leading to possible delays during emergencies. 2. Even if such a spectrum is developed, disaster-prone areas are often fragile and it is the telecom infrastructure which is most frequently disrupted in such cases. 3. Operational coordination between DoT and MHA can be slow and and unclear during emergencies.	1. The policy can recomment collaborations between MHA and DoT to explore such spectrum particularly to be used only for PPDR needs. 2. The policy can propose the development of reliable infrastructure models such as satellite backup to be deployed post-disaster. 3. A dedicated PPDR Coordination Cell may be created to ensure that during real-time emergencies, there is swift action.
	1.4. Adopt intelligent, integrated and data-driven infrastructure planning through initiatives like Digital Twin in various sectors;	1. The current quality of data ecosystems consisting the data of multiple departments like power, transport, etc. is often outdated which will make it very difficult to implement such an initiative. 2. The implementation of Digital Twin systems, especially in cities	1. A standardized framework for data-sharing can be proposed in the policy wherein infrastructure-related data can be shared on a common platform. 2. The policy can propose the implementation of such a system in a phased manner, beginning

		that are not Tier 1, can be very expensive.	with Tier 1 cities as models and then move on to Tier 2 and 3 cities so that by then the costs and problems can be identified.
	1.5. Explore the possibility of segregation and rationalization of compliances for retail and enterprise businesses.	1. There are often complications in understanding which provisions would exactly apply to which business. It is not only the segregation of compliances that is necessary, but a clear division between business is necessary. 2. Another thing that is missing is that there are a lot of redundant and overlapping reporting requirements that must be filed.	1. The policy can propose the possibility of clearly dividing businesses into certain categories and then framing laws according to that to ensure that there is no confusion as to which law would apply to whom. 2. The policy can recommend streamlining compliance forms through a possible unified reporting platform.
(2)	2.1.Streamline grievance redressal process through unified portal and use of AI, Chatbots etc.	1. Currently, each telecom company has its own complaint portal which has led to a scattered complaint system. 2. The usage of digital grievance redressal tools, especially the use of AI and Chatbots may be too difficult to use for users from rural-areas and low income groups 3. Moreover, the usage of AI can be useful only in cases that do not require human interaction. In some escalated cases like fraud cases or billing disputes, there is a need of a human touch. 4. There is a possibility of	1. The policy can propose a National-level grievance redressal portal which would be integrated with individual service providers. 2. The policy can recommend that the portal and AI tools should use voice-based inputs, which would ensure accessibility. 3. The policy can suggest the use of AI models in such a way that the escalated disputes are automatically raised to human agents. 4. The policy can promote the development of a real-time tracking system so that users can

		dissatisfaction with the system due to the absence of real-time tracking systems of one's complaint.	monitor at what stage their complaint is in the resolution process.
	2.2. Promote unified information system for all telecom services in vernacular languages	1. Even if such vernacular systems are created, users may not know that they exist, especially in rural areas, where word-of-mouth is of greater importance.	1. In addition to these systems, the policy can propose additionally that there should be a Information, Education and Communication (IEC) campaign through local bodies that will ensure that there is wide-spread awareness of such systems.
	2.3. Enhance awareness to address the concerns of citizens related to EMF radiation of telecommunications towers	1. Currently, government explanations are filled with technical terms and guidelines that are difficult to understand, which are a major cause of these concerns. 2. In practicality, information coming from telecom companies may be viewed with suspicion.	1. The policy can propose easy-to-understand videos in multiple languages, and perhaps even infographics that would make it easier to address the concerns of the public. 2. The policy can suggest collaborations with local media professionals to enusre the dissipated information is trusted.
	2.4. Create a single window support system for resolving issues pertaining to telecommunications sector	1. There is low awareness amongst the stakeholders as to how or where to raise issues even if a single window support system is created. 2. If this window is not well-managed, then it could become a bottleneck that would delay rather than speed up the resolution	1. The policy can suggest measures to raise awareness amongst the general public about this system. 2. Instead of a single window support system, there can be a centralized dashboard where all issues are registered, and then these issues based on their

		process. 3. Further, there might be a resistance to this change as some departments might fear losing control and hence want to work independently.	categories can be rerouted to the department that is responsible. 3. The policy can suggest that this system, if implemented, should be rolled out in a phased manner.
	2.5. Organize capacity-building programs for Central Ministries, States and public institutions like Districts, Schools, Colleges etc. on 5G and BharatNet use cases	1. Different sectors may have and may need different levels of capacity-building and awareness, and a general framework would be difficult to follow for everyone. 2. Such capacity builiding programmes, in reality, are often a one-time event with no follow ups, which leads to even more confusion in the minds of the public.	1. The policy can suggest capacity-building programmes that are suited specifically to the groups they are addressing. 2. The policy can recommend the setting up of these programmed in a phased out manner to ensure that follow up sessions are done and the concerns of the public are resolved.
	2.6. Encourage pilot projects related to use cases of 5G and BharatNet network	1. There is often a limitation as to funding for pilot projects. 2. The collaborations that are needed for such pilot programmes are often weak in this sector. 3. There is also difficulty in scaling successful pilot projects into nation-wide programmes.	1. The policy can suggest a grant programme or innovation challenge funds to support such small scale pilot programmes that can also be co-financed by government. 2. Public Private Partnership (PPP) Model can be suggested for these pilot programmes where the DoT can facilitate a sort of matchmaking between such programmes and those who can finance them. 3. A fast-track adoption pathway

			can be set up for such pilot programmes so that they are implemented quickly.
	2.7. Scale up the successful pilot projects at pan-India level including Samriddh Gram	1. Some pilots that have worked in one particular area may not necessarily work in other areas. 2. The problem with scaling up the successful pilot projects also lies in the funding requirements as substantial amount of capital is required for operational funding. 3. Coordination accorss various stakeholders can also pose a challenge when a pilot project is implemented at a larger scale.	1. Regional adaptation models can be incorporated during a scale up (when these successful pilots are expanded at a pan-India level). 2. The policy can also encourage blended financial models to ensure this scale up that combines state and national budgets, as well as possible contributions from the USOF allocations. 3. The policy can suggest the setting up of a National Scale Task Force to implement these pilot projects.
(3)	3.1. Develop end-to-end online solution for all compliance reporting, encouraging self declarations wherever possible	1. One problem that may arise is that currently the compliance processes are fragmented across various departments, which can lead to confusion since they all have different portals and formats. 2. Authorities may hesitate to accept self-declarations due to concerns about accuracy or misuse. 3. There may be difficulty using these online systems for smaller players in the market since they may not be aware of the process	1. The policy can recommend the setting up of a single national online platform for all compliance requirements that have to be complied with so that they can be accessed at one place and ensuring compliance will become easier as well. 2. Self-declarations can be made mandatory only for low-risk entities, and for high-risk entities proper and detailed audits may be done to ensure compliance. 3. Training and capacity-building

		owing to lack of training.	programmes can be done for these small level players so that they are able to integrate well into the system and do not fail to comply with the requirements.
	3.2. Collaborate with states and UTs and Ministry of Power through NBM institutional framework to implement composite billing system for all TSPs/ISPs/IPs	1. In the current practical scenario, telecom operators and electricity providers maintain separate and unlinked databases due to which there can be a mismatch and billing disputes. 2. There can be some resistance from State Electricity Boards to this scheme since they may fear losing control or may fear system overhaul costs. 3. Integrating such billing systems would mean that sensitive information of financial and operative data has to be shared which may be at risk.	1. The policy can suggest a shared digital platform where both of these entities can upload consumption data in real time which will eventually reduce delays and errors. 2. Propose pilot projects in some states that will demonstrate cost savings and efficiency gains for utilities. This will build trust and reduce resistance. 3. The policy can recommend incorporating secure data exchange protocols, encryption, and role based access control if there is a composite billing platform.
	3.3. Promote use of RegTech and code-based modalities	1. A lot of telecom operators who are smaller players in the industry are unaware of what is RegTech and how RegTech may simplify compliance. 2. There is often a high cost of adoption of such technology due to the investment that has to be made in software, integration and	1. An awareness drive which would include programmes and workshops can be arranged which will showcase how RegTech can be used. This will help to ease the smaller players into the system. 2. The policy can promote shared RegTech platforms or government-supported cloud-

		training.	based compliance tools. This will reduce per-operator costs and allow gradual onboarding.
	3.4. Explore the possibility of deemed approval beyond prescribed time limits for different regulatory and licensing/authorization activities within the department	1. One of the biggest problems with this provision is that if deemed approvals are granted automatically then applications with errors or missing documents might get cleared without proper checks. 2. Some authorizations in the telecom sector also involve things like security clearances, spectrum assignments, cross agency approvals, etc. which cannot be fast tracked legally since they require time to be processed and checked. 3. Moreover, if the above two problems are not taken care of, people may misuse this system and submit incomplete applications on purpose and get deemed approval for them. This would be really risky to the system as a whole.	1. The policy can suggest a pre-screening mechanism where the applications have to be vetted for completeness before the clock for deemed approval starts so that there is no risk of incompleteness. 2. If the deemed approval system *has* to be introduced, then perhaps there can be a categorization of applications wherein deemed approvals can only be given on low-risk and routine approvals such as renewal of an existing license, for example. 3. In such a case, one possible solution is conditional deemed approvals whereby the authorization is held valid but if violations are found post a detailed audit, then the authorization will stand revoked.
	3.5. Promote active and passive infrastructure sharing and implement regulatory framework for the same.	1. There can be some commercial reluctance to share infrastructure due to the competetive advantage that they may want to maintain. 2. Different operators may also	1. The policy can promote incentive based sharing models whereby operators benefit through cost reduction, particularly in spectrum allocation and other such things if they participate in such

		use different non-compatible network equipment which would make active sharing difficult.	sharing arrangements. 2. The policy can promote common technical standards and interoperability guidelines for shared infrastructure. These guidelines ought to be developed in consultation with industry bodies.
	3.6. Conduct study on Regulatory Impact Assessment for improvement of regulatory environment and practices	1. Regulatory Impact Assessments require reliable data on the effects of past regulations, but such data is often incomplete or unavailable in the telecom sector. 2. Moreover, over time, these RIAs may become a mere box to tick and will not be translated into actual changes.	1. The policy can propose the development of a centralized data depository that tracks the performance and market impact of each provision over time. 2. To prevent this, the policy can suggest public disclosure of these assessments to ensure adherance and to ensure that changes are made according to the results.
	3.7. Develop framework to enable and encourage spectrum sharing, leasing, trading and secondary usage Ensure adequate availability and efficient utilisation of spectrum through refarming	1. If there is spectrum trading and leasing, there is a possibility that it will lead to market concentration since large operators will accumulate excess spectrum and this will reduce active and healthy competition. 2. Further, if this spectrum sharing is not managed properly, then it can lead to interferance which will impact the quality of the service.	1. The policy can introduce spectrum caps and anti-hoarding provisions in the framework to prevent dominance by a few players. 2. The policy can promote technical coordination standards and monitoring systems to manage such interference.
	3.8. Undertake spectrum audit of Central, State	1. Some ministries and state departments, or even PSUs may	1. The policy can propose a confidential audit mechanism

	Government and PSUs on regular basis	be reluctant to share usage data due to security concerns or institutional control concerns. 2. Accurately tracking actual spectrum use requires specialised monitoring equipment and skilled personnel which may not always be available.	whereby sensitive information is reviewed securely, and only non-sensitive findings are shared. 2. The policy can promote investment in spectrum monitoring infrastructure and training programs for technical staff to ensure good audits.
	3.9. Delegate the frequency assignment activity to the regional level to enhance accessibility and expedite spectrum allocation for wireless users	1. Regional offices might apply the spectrum assignment rules differently which can cause uneven treatment of applicants. 2. Decentralisation may also cause confusion over frequency availability or overlaps.	1. The policy can propose uniform training for all regional offices to ensure that the decisions that are made are consistent throughout the nation. 2. The policy can recommend establishing a centralised frequency database that will be accessible to both central and regional offices to prevent conflicts and duplication.
	3.10. Ensure adequate availability and efficient utilization of spectrum through refarming	1. Shutting down old networks for refarming requires moving customers to newer technologies. This can be complicated and time-consuming. 2. Many users still use older devices that cannot support newer networks, which makes them vulnerable during refarming. 3. Existing licenses and agreements may have technology-specific clauses that slow down	1. The policy can encourage phased migration plans with public awareness campaigns to prepare users in advance. 2. The policy can propose subsidy or exchange programs to help users upgrade to more compatible devices. 3. The policy may recommend updating license conditions to allow technology neutrality, so that the spectrum can be used

		the reallocation process.	fresh approvals.
	3.11. Develop a dynamic National Spectrum Roadmap updated every two years, aligned with ITUR WRC cycles and industry needs	1. In practicality, telecom technologies evolve very rapidly which makes it hard to forecast spectrum needs several years ahead. 2. Spectrum planning involves a lot of authorities including but not limited to DoT, TRAI, Defence, Broadcasting and state authorities, which can lead to delays in finalising the roadmap.	1. The policy can propose to adopt flexible spectrum planning models that allow mid-cycle adjustments based on technological breakthroughs. 2. The policy can propose to set up a permanent inter-agency spectrum coordination body to streamline decision-making and align interests.

MISSION 6

Strategy No.	Provision	Issues Identified	Proposed Solutions
(1)	1.1. Encourage the use of AI-enabled management system to optimize energy consumption	1. AI energy management systems requires a lot of investment which can be expensive for smaller operators. 2. Another problem that may arise is that it can be difficult for older telecom systems to interface with these new AI Based systems, making it difficult to optimise energy usage. 3. The usage of AI systems may lead to cybersecurity concerns.	1. The policy can encourage public-private funding models or subsidies to help telecom operators adopt AI tools without heavy investment costs. 2. The policy can promote the adaptation of these AI systems in a phased manner, integrating them into the newer systems first. 3. The policy can mandate secure data handling protocols, encryption, and periodic vulnerability testing for AI energy systems.
	1.2. Facilitate the implementation of "Green Energy Open Access" framework by collaboration with States and UTs for enhancing the use of green/renewable energy in the telecom sector	1. Different States and UTs may have differing rules, charges, and approval processes for open access to renewable energy. This would make it difficult to implement it nation-wide. 2. Some sources of green energy such as water and wind can be unreliable and they can disrupt the telecom sector.	1. The policy can encourage the creation of model state-level policies aligned with the national framework to ensure uniformity and predictability. 2. Hybrid energy models can be promoted to ensure continuous flow of energy to the telecom sector.
	1.3. Facilitate continuous	1. One major issue that may arise	1. The policy can promote the

	reduction in carbon footprint from the telecom sector by educating and incentivizing suppliers and customers, as well increasing the product lifecycles of telecom equipment.	is that eco-friendly materials, processes, and recycling systems often cost more than conventional methods. 2. Without standardised metrics, it's hard to verify real environmental impact.	offering of financial incentives, tax credits, or preferential procurement policies for suppliers who meet defined sustainability benchmarks. 2. Adopt uniform carbon accounting frameworks for the telecom sector, with mandatory annual reporting and third-party audits.
	2.1. Encourage and incentivize the design of products and services, conforming to Circular Economy principles and efficient green energy technologies	1. One of the biggest issues is that Cirular Economy designs that are repairable and recyclable often cost a lot more to develop than traditional models. Further, many customers still prioritize cost over green energy and they would want to buy cheaper services rather than going for a sustainable service. 2. Another issue is that the impact of circular designs can be hard to quantify and compare across products.	1. One possible solution is offering grants to such designs, or reducing import duties on eco-friendly materials to offset the higher production costs. As such, when the cost of the commodity is low, the consumers can also buy that rather than avoiding sustainable material. 2. The policy can recommend life-cycle assessments (LCA) for telecom products.
	2.2. Facilitate product stewardship programs that ensure responsibility for the entire product life cycle, including end-of-life disposal, through collaboration among	1. End-of-life products often do not reach authorised recyclers due to poor collection systems. 2. Consumers often discard devices improperly because returning them is inconvenient	1. The policy ought to encourage solid collection networks and drop-off points for telecom waste at retail outlets and service centres. 2. The policy can introduce deposit–refund or buy-back

	governments, businesses, and consumers	and unrewarded.	schemes where customers receive monetary or service benefits for returning old devices.
	2.3. Develop National Standards for promoting circularity for telecommunications sector, aligned with the internationally recognized standards	1. Such strict standards may burden smaller telecom equipment makers who do not have the resources to ensure compliance. 2. Another problem is that if there is a misalignment with international standards, it could lead to a decline in exports. 3. Many manufacturers may not know how to integrate circular principles into their production processes.	1. A possible solution to this is to introduce a three-tiered compliance system, such that there are lower degree of norms to follow for smaller enterprises, and more strict norms for larger enterprises who have the means to follow these norms. 2. The policy can suggest an alignment with international guidelines such as ITU, ISO or IEC standards, and also an active participation by India in international standardization committees. 3. The government can offer training programs and technical manuals to guide telecom companies in meeting new national standards.
	2.4. Introduce e-waste recycling mandates for telecom manufacturing companies, encouraging manufacturers to adopt Circular Economy models by reusing and recycling telecom equipment	1. Setting up authorised e-waste recycling facilities is expensive and may discourage smaller manufacturers. 2. Currently, a lot of the telecom sector waste is handled by informal contractors who use unsafe methods to deal with it.	1. The policy can promote shared recycling facilities which may be funded by government incentives. 2. The policy can suggest as a solution formal recycling chains through training, certification, and partnerships with authorized recyclers that currently work.

		3. Most consumers do not return old devices due to lack of any sort of reward or incentive.	3. A system like a deposit-refund system, or exchange schemes can be implemented so that consumers are encouraged to return old devices and they are not dealt with improperly as waste.
	2.5. Promote R&D in areas of sustainability and Circular Economy in Telecom Sector	1. Currently, the R&D budgets that are already in place focus on network expansion and performance rather than sustainability. 2. Even where R&D efforts are successful, it does not reach the market due to not having support for scaling.	1. The policy can recommend the creation of dedicated R&D budgets specifically for researching upon sustainability. The funding can be done by not only the government but industry giants as well. 2. The policy can recommend innovation-to-market programmes that offer prototype funding and regulatory fast-tracking for such green telecom solutions.
	2.6. Incentivize telecom products conforming to circularity in public procurement	1. Such sustainably designed products may cost more initially which will make them less competitive compared to other tenders that come through public procurement.	1. The policy can adopt lifecycle cost evaluation in tenders, whereby lower long-term operating and disposal costs are factored into the selection criteria, so that such products also have a chance of being selected.
	2.7. Incentivize telecom products conforming to circularity through suitable enabling modifications in the existing DoT Schemes and new schemes	1. There is currently a lack of clear, measurable indicators of whether or not a product conforms to circularity. Thus, it's hard to tie incentives reliably to circular performance.	1. The policy can recommend development of simple and tiered circularity metrics linked to existing standards. Further, these tiers can be used to map to give larger benefits for higher tiers so

		2. Firms could claim circular features to access incentives without substantive design change or verification.	that there can be a balance between funding and the development of such infrastructure. 2. The policy can advise introducing mandatory third-party certification and periodic audits as a condition for getting the incentive.
	2.8. Develop courses on Circular Economy in Telecom, in association with AICTE and other academic/ industry experts, for engineering colleges, polytechnics, ITIs, etc.	1. Currently, teachers may lack knowledge of sustainability principles specific to the telecom sector.	1. Introduce faculty development programs and industry-led training workshops to equip educators with updated skills and case studies.
	2.9. Promote the use of refurbished products that have similar level of warranty support from vendors	1. Many consumers may think that such refurbished products are less reliable than newer ones. 2. From the point of view of the vendors, they may hesitate to provide warranty to such products since there is a perceived higher risk of these products getting damaged easily. 3. Without clear guidelines, as is the situation currently, refurbishment quality can vary widely, affecting performance.	1. The policy can recommend awareness campaigns and also possibly require these products to have quality certification labels to put the minds of buyers at ease. 2. The government can offer incentives or a shared-warranty system to encourage vendors to match warranties. 3. The policy can recommend a national standard for refurbishment.
	2.10. Coordinate with Department of Consumer	1. Some manufacturers may be reluctant to share repair manuals	1. Negotiate balanced disclosure rules, allowing access to necessary

	Affairs for on boarding of Telecom Equipment on the Right to Repair Portal	or parts, citing intellectual property protection or safety risks. 2. Repair manuals, software tools, and parts catalogues may come in different, incompatible formats.	repair information while protecting proprietary designs and safety guidelines can also be included in this 2. The policy can recommend creating standardised digital formats for repair documentation and integrating them with the Right to Repair Portal.
	2.11. Formulate rating framework for telecom infrastructure resilient to climate change and incentivize its adoption	1. Resilient designs may require stronger materials, elevated structures, or backup systems, increasing costs.	1. The policy can recommend offering capital subsidies, tax benefits, or low-interest loans for companies investing in climate-resilient upgrades.
	2.12. Establish a Centre of Excellence (CoE) on "Sustainability in Telecom Sector"	1. This CoE would need significant initial and ongoing investment for infrastructure, experts, as well as R&D activities. 2. If the industry giants see the CoE as something purely academic, then they might not actively engage with it.	1. The policy can recommend multi-source funding like from government grants or contributions from the industry itself. 2. The CoE can be designed in a public-private partnership model with industry giants chairing advisory boards.
	2.13. Collaborate/facilitate relevant ministries/departments for a resilient Public Protection and Disaster Relief (PPDR) network with harmonized	1. There is no dedicated and uniform pan-India spectrum explicitly set aside for PPDR needs that may arise, leading to possible delays during emergencies.	1. The policy can recomment collaborations between MHA and DoT to explore such spectrum particularly to be used only for PPDR needs. 2. The policy can propose the

	spectrum plans, AI-powered predictive analytics, and IoT-enabled systems for resource mobilization	2. Even if such a spectrum is developed, disaster-prone areas are often fragile and it is the telecom infrastructure which is most frequently disrupted in such cases. 3. Operational coordination between DoT and MHA can be slow and and unclear during emergencies.	development of reliable infrastructure models such as satellite backup to be deployed post-disaster. 3. A dedicated PPDR Coordination Cell may be created to ensure that during real-time emergencies, there is swift action.
	3.1. Promote energy efficiency at component, equipment/system and network/service level through energy consumption rating and classification of energy passport	1. One major problem that may be faced is that currently, there is no accepted benchmark for rating telecom components or systems in India. 2. The industry players may see this as extra burden and paperwork, and may not prioritize these energy ratings.	1. The policy can recommend the development of a national energy efficiency standards for telecom equipment. 2. The government can provide subsidised testing facilities and simplified digital filing systems to make compliance easier and cheaper. Further, they can mandate public procurement preference for high-rated products and run awareness campaigns on long-term savings.
	3.2. Promote the use of renewable energy sources for powering telecom network	1. One major problem can be that installing renewable energy systems, especially for large-scale telecom infrastructure, can require significant capital investment. 2. Solar and wind energy availability varies by time and weather, which can disrupt	1. Encourage green financing models, tax incentives, or public-private partnerships to lower the initial financial burden. 2. The policy can promote hybrid energy solutions that combine renewable sources with backup diesel generators for reliability.

		continuous network operations. 3. In dense city locations, limited rooftop or land space may make large renewable installations difficult.	3. Encourage shared renewable energy infrastructure among multiple telecom operators in urban areas.
	3.3. Ensure capacity building in educational institutions.	1. Most educational institutions do not include sustainability-focused telecom modules in their existing courses. 2. Institutions often work in isolation from the telecom industry, reducing practical exposure for students.	1. Collaborate with AICTE, UGC, and technical universities to develop dedicated courses, certifications, or electives on green telecom technologies. 2. Create internship, mentorship, and live project programs where students work directly with telecom companies on sustainability initiatives.