COAI

COAI Additional /Counter Comments on the Consultation Paper on “Digital Transformation through 5G Ecosystem”

1. We thank the Authority for providing us with the opportunity to share the additional/counter comments to the Consultation paper on Digital Transformation through 5G Ecosystem. Given the rapid advancement of new technologies, particularly in relation to the development of virtual worlds and the metaverse, we believe that the decision to initiate a public dialogue will go a long way in ensuring that such technologies are able to meet their full potential.

2. India's economy and society are being drastically altered by the country's rapid digital development. The advent of 5G technology signifies a substantial transformation, signifying the start of an era in which the digital revolution infiltrates every facet of our existence and societies. The fifth-generation technology ecosystem plays a crucial role in facilitating a range of transformational developments that possess the capacity to redefine connectivity, efficiency, and accessibility.

3. There is no doubt that the 5G services, its ecosystem and use cases will play most crucial role in driving digital transformation across various industries by providing faster and more reliable connectivity. 5G with its faster data speeds, increased bandwidth, and lower latency, will provide businesses and innovators with the connectivity and capabilities that can give wings to their dreams.

4. 5G applications or 5G triangle comprising of eMBB (Enhanced Mobile Broadband), mMTC (Massive Machine Type Communications) and uRLLC (Ultra-Reliable and Low Latency Communications) are poised to revolutionize all sectors of economy.

5. 5G technology represents a monumental leap in wireless communication, poised to revolutionize the way we interact with the digital world. This next-generation technology offers exponentially faster data speeds, remarkably reduced latency, and the capacity to connect a vast number of devices simultaneously, paving the way for innovations in fields like autonomous vehicles, smart cities, and IoT (Internet of Things). Telecom service providers globally have heavily invested in 5G infrastructure, recognizing its potential to transform not just mobile communications, but also to catalyze advancements across various sectors. Their commitment is evident in the extensive rollout of 5G networks, massive research and development efforts, and collaborations with tech industries to unlock the full potential of this groundbreaking technology.

6. In India the TSPs have invested more than Rs. 1 Lakh Crores in creating a robust 5G Infrastructure, however there are still challenges related to the monetisation of the 5G services, since there a limited use case for the 5G services. Having no use cases for the

5G is in fact global issue. All over the world TSPs are unable to recover the amount of investment made in creating a 5G network.

7. Further, TSPs are still facing the policy and regulatory related challenges for providing the 5G services other than the lack of established use cases is affecting wider adoption of 5G services.

8. Some of the challenges with respect to the Digital Transformation through the 5G Ecosystem are related to the policy & regulatory restrictions w.r.t M2M Services, Challenges in the implementation of RoW Rules by the state Government, Municipalities, Central Government agencies etc & high RoW charges being levied for the deployment of fibre and regulation related to Network slicing.

9. Further, it is important to note here that the current EMF exposure limits in India are significantly stricter (10 times) than the ICNIRP norms, and if not revised, will severely harm consumer experience and expectations from 5G in India. This will adversely deteriorate 5G leading to slower internet speed, lower network quality and inferior signal strength. In addition, this will also impact all potential aspects to enhance the wireless infrastructure and deployment of 5G, including spectral efficiency and network topology.

10. Also, restriction has been imposed by DoT based on DGCA recommendations mandating large exclusion zones for 5G/IMT base stations in 3300-3670 MHz bands for Aircrafts, prescribing no C-band zone of 2.1 KMs from both ends of the runway and 910 meters from center of the runway. These Directives have an impact on the deployment and availability of 5G services at airports, airstrips, helipads, etc. as well as adjoining areas across the country**.**

11. As per the estimates 5G technology in India is projected to make a cumulative economic **impact of $1 trillion by 2035**, however, would need a concerted effort by the industry as well as government authorities to clear the roadblocks and hasten adoption of the technology.

12. To this end, we have provided our responses and recommendations below. We note that several issues and legal questions posed in the Consultation Paper may not fall within TRAI's regulatory ambit. We have provided our recommendations with the expectation that it will serve to inform all relevant ministries and stakeholders towards a common aim.

13. It is with this background in mind that we provide our response to questions raised by the TRAI in the paper.

Q.1. Is there a need for additional measures to further strengthen the cross-sector collaboration for development and adoption of 5G use cases in India? If answer is yes, please submit your suggestions with reasons and justifications. Please also provide the best practices and lessons learnt from other countries and India to support your comments.

COAI Response:

1. A collaborative partnership between the public and private sectors has the potential to accelerate the implementation of infrastructure projects. The government has the capacity to offer various incentives, while private businesses possess specialised technological knowledge and skills. We must acknowledge the necessity of transitioning away from regulatory interventions and policies that are considered and executed in isolation inside a single agency or ministry. We believe that in order to further strengthen the cross-sector collaboration for development and adoption of 5G use cases in India, additional measures need to be undertaken.

2. The details provided in the Consultation paper indicate that the Government, the Authority, and all concerned ministries are already collaborating to identify and promote India specific 5G use cases in different industry verticals like Healthcare, Education, Governance, Banking, Finance, Insurance, Cyber Security, Enterprise transformation, Industry 4.0, Agriculture, Livestock, Smart Cities & Infrastructure etc. The "5G Hackathon" has been yielding some good ideas and more is expected in subsequent phases starting with Phase 2.

3. The fact that the Government of India is setting up 100 test labs in collaboration with 14 other ministries and departments viz. Ministry of Mines, Ministry of Power, Ministry of Agriculture, Ministry of Education, Ministry of Urban Development, Ministry of Railways, Ministry of Road Transport and Highways, Department of Water, Ministry of Tourism, Ministry of Heavy Industries, Ministry of Health and Family Welfare, Ministry of Housing and Urban Administration, Ministry Electronics and IT, and the Department of Science and Technology to explore 5G use cases indicates that the efforts are already underway at Government and Regulators level to facilitate the cross-sector collaboration and development of 5G use cases in the country.

4. In furtherance to the above, the following suggestions can be taken into consideration:

   a. Facilitate and encourage interdisciplinary research partnerships among technology enterprises, academic institutions, and government research facilities. It is recommended to allocate funds and incentives to support the development of groundbreaking breakthroughs.

   b. Encourage the understanding of the practical applications in different industries.

c. Address obstacles related to Right-of-Way (RoW) concerns i.e. all the States, Municipal Corporations and central agencies adopt the Indian Telegraph RoW rules released by DoT in 2018 and the amendments thereafter.

d. Restrictions in the implementation of the technologies under 5G should be removed e.g. restrictions of 4 URLs for the M2M services. These restrictive features may be analysed comprehensively taking into account service need aspects without sacrificing essential security consideration. Considering global nature of these services, the best international practices may also be studied to come up with the comprehensive solution.

e. Establish partnerships with educational institutions to provide a specialised curriculum focused on 5G technology. This practise guarantees the presence of a proficient labour force capable of effectively carrying out tasks related to deployment and maintenance.

f. Provide incentives for creating the robust 5G infrastructure in the country for e.g. provide subsidies for the deployment of 5G infrastructure in rural areas to ensure that the setup cost does not become a barrier to access.

g. A central agency, encompassing representatives from government, industry, academia, and civil society, could foster collaboration, define priorities, and allocate resources efficiently.

h. Create standardized frameworks and APIs: Establishing common guidelines and application programming interfaces will ensure interoperability of solutions and facilitate their adaptation across different industries.

i. Promote joint pilot projects: Encourage and incentivize collaboration between diverse stakeholders to test and refine 5G solutions for real-world challenges. This fosters knowledge exchange and builds confidence for wider adoption.

j. Invest in skill development: Upskilling programs tailored to 5G use cases should be offered to professionals across sectors, including engineers, entrepreneurs, and policymakers.

k. Leverage international best practices: Learn from the successes and challenges of countries like South Korea and Germany in their 5G journeys. Adapt their models to suit the Indian context.

l. Include representatives from key sectors like healthcare, education, and manufacturing. A dedicated task force will ensure that all sectors are aligned in their approach towards adopting and leveraging 5G. It facilitates the sharing of insights, resources, and best practices, ensuring that 5G implementation is efficient and cohesive across various industries. It also helps in ensuring uniform adoption across sectors and fostering innovation through collaborative efforts.

m. Facilitate collaboration and idea-sharing between industries - Innovation summits bring together leaders from various industries, academia, and government, fostering a collaborative environment. They serve as platforms for discussing challenges, sharing ideas, and showcasing new technologies. They also promote knowledge exchange, encourages joint ventures, and helps in identifying and solving sector-specific challenges with 5G.

Best Practices and Lessons Learnt:

a. South Korea: Their focus on early spectrum allocation, public-private partnerships, and open innovation ecosystems facilitated rapid 5G deployment and diverse use cases.

b. India: Early pilots in areas like smart cities and healthcare have shown promise. The focus should be on scaling these up and fostering horizontal collaboration across sectors.

c. Finland's 5G Momentum ecosystem encourages collaboration through regular events and workshops, bringing together various stakeholders. 5G Momentum ecosystem makes Finland a pioneer in 5G | Traficom Finland working in international cooperation towards future technologies - FiCom[1]

Q.2. Do you anticipate any barriers in development of ecosystem for 5G use cases, which need to be addressed? If yes, please identify those barriers and suggest the possible policy and regulatory interventions including incentives to overcome such barriers. Please also provide the details of the measures taken by other countries to remove such barriers.

COAI Response:

1. First and foremost, ecosystem for 5G use cases is contingent on the massive and dense deployment of 5G in the country. Only dense and ubiquitous availability of 5G will help realize the full potential of 5G use cases across sectors and industries.

2. The development and deployment of 5G technology is not without challenges. The complex nature of the 5G ecosystem, coupled with the unique requirements of different markets, presents a series of barriers. Despite the immense potential of 5G, several roadblocks hinder the development of a robust ecosystem for its use cases in India. Addressing these

[1] https://ficom.fi/news/finland-working-in-international-cooperation-towards-future-technologies/

barriers through targeted policy interventions and incentives is crucial for unlocking the technology's transformative power. They are as follows:

a. Due to the nature of 5G's high-frequency spectrum, it requires denser infrastructure, including many small cells and base stations. Deploying these in urban areas might be feasible, but it becomes challenging in rural or less densely populated regions.

b. Further, Infrastructural development is crucial for 5G deployment. Grants can stimulate investment in necessary hardware, such as cell towers and fiber optics, especially in rural and underserved areas. Encourage development in regions that may not be immediately profitable for private companies.

c. The U.S. Federal Communications Commission's (FCC) Rural Digital Opportunity Fund allocates funds to build and maintain infrastructure. Auction 904: Rural Digital Opportunity Fund | Federal Communications Commission (fcc.gov)[2]

d. 5G requires widespread fiber optic backhaul (more specific to mmWave / small cell) and dense cell site deployment, which are currently lacking in many parts of India. This limited infrastructure creates bottlenecks for seamless connectivity and wider coverage.

e. Lack of standardization and interoperability: The absence of standardized frameworks and application programming interfaces (APIs) creates challenges for developers. Adapting solutions to diverse infrastructure and industry needs becomes complex and time-consuming.

f. DoT, GoI had notified the Indian Telegraph Right of Way 2016 Rules in November 2016 (RoW rules), the same has been amended on regular basis. It was envisaged that all the States and Union Territories will issue rules, policies, orders aligned with the RoW rules, However, the pace of alignment of Right of Way Rules across all States/UTs and Central ministries is a concern. The RoW rules should be adopted and implemented in letter and spirit, especially by the local authorities in the states and UTs, which have their own bylaws and guidelines.

g. NBM has created an online portal, Gati Shakti Sanchar, for processing applications for permissions related to deployment of towers and OFCs (underground and overground). This ease of business initiative is still to give complete benefits since integration of all State level and Local authorities' portals with the Gati Shakti portal has not happened.

h. As the country progresses and its infrastructure improves, it is important that facilitation for creation of common ducts in the cities to blow fiber should be prioritized.

[2] https://www.fcc.gov/auction/904

Governments could ease regulations related to infrastructure deployment and further public-private partnerships can be formed to share the infrastructure burden.

i. As the network elements come nearer to the users, in-building solution and Digital Connectivity within houses, buildings, public spaces (airports, malls, railway stations etc.) is critical. Ministry of Home and Urban Affairs (MoHUA) has issued an amendment to Building Bylaws, the same needs to adopted by the states and UTs immediately.

j. DoT has permitted the use of 865-868 MHz for "Tracking, Tracing and Data Acquisition Devices" and "Radio Frequency Identification Applications" without acquiring a license. It is to be noted that allowing unlicensed frequency bands for deploying a critical application like Advanced Metering Infrastructure (AMI) at a wider scale will seriously compromise the security of the critical infrastructure apart from leading huge revenue loss to the Government and thus, such a critical application/infrastructure should be created only by the telecom companies under their license and over the licensed spectrum.

k. Telecom is a main component of any IT ecosystem and accordingly inclusion of telecommunication in all states IT/ITES policies is mandatory. All benefits extended to this sector by the state governments need to be extended to the telecom too.

l. Availability of Government assets like Land, Buildings, Street Furniture will give big boost for improving connectivity. The same should be provided in timely manner in minimum / nil cost for proliferation of telecom in their territories.

Lessons from other countries:

a. South Korea: Their focus on government-backed infrastructure projects, and open innovation ecosystems facilitated rapid 5G deployment and diverse use cases.

b. Singapore: Their emphasis on collaboration, talent development, and regulatory sandboxes to test innovative solutions fostered a thriving 5G ecosystem.

Q.3. What are the policy measures required to create awareness and promote use of 5G technology and its infrastructure so that the citizens including those residing in rural and remote areas may benefit from the 5G use cases and services to create new economic activities and increase employment opportunities and thereby promote economic growth of the country?

COAI Response:

1. Creating awareness and promoting the use of 5G technology is essential for leveraging its full potential to drive economic activities and employment opportunities, especially in a

country as diverse and geographically expansive as India. In this regard, we suggest the following policy measures to be taken by the Government:

a. Policymakers should aim to invest in providing the infrastructure, capacity building and awareness programmes for creating awareness among the citizens and provide a conducive environment for adoption and promotion of these use case.

b. Launch national-level campaigns to educate citizens about the benefits and opportunities of 5G. These should be in multiple languages and accessible formats to ensure wide understanding.

c. Implement training programs in rural and remote communities to demonstrate 5G use cases. For example, show how 5G can help in agriculture, telemedicine, and education.

d. Offer financial incentives or tax breaks to companies that develop 5G applications tailored to local needs, such as apps for local language content, e-health services, and e-learning.

e. Work with local governments to identify the most pressing needs of their communities that 5G can address, creating a demand-driven approach to technology adoption.

f. Set up 5G innovation centres or hubs, especially in universities and technical institutes, to encourage young entrepreneurs and tech enthusiasts to experiment with 5G technology.

g. Encourage creation of content and services that cater to the specific interests and needs of rural populations, making 5G services more relevant.

h. A major barrier to 5G adoption is the lack of awareness and understanding of its benefits and applications, especially in rural and remote areas. Educate citizens about the benefits and uses of 5G by running literacy campaigns tailored around 5G & its application benefits. Customize campaigns to address specific regional needs and language barriers. Use a mix of traditional and digital media to reach a wider audience.

   i. Singapore’s Smart Nation initiative focuses on increasing digital literacy and public awareness of new technologies.[3]

   ii. Australia’s Regional Tech Hub is another example. Regional Tech Hub improving digital literacy for rural Australians[4]

[3] https://www.smartnation.gov.sg/about-smart-nation/transforming-singapore/

[4] https://www.rowanramsey.com.au/regional-tech-hub-improving-digital-literacy-for-rural-australians/

i. The high cost of 5G-enabled devices and services can be prohibitive, especially in underprivileged, lower-income and rural areas. Implement or provide subsidy schemes for handsets in proportion of market share..

j. There is a need to educate not just the public but also businesses and local governments about the potential applications and benefits of 5G. Host workshops and training programs for small businesses and local government officials. Develop online resources and training modules accessible nationwide.

i. Finland's 5G MOOC (Massive Open Online Course) provides comprehensive knowledge about 5G technology to a broad audience[5].

Q.4. What are the policy measures required to promote use of IoT technology and its infrastructure so that the citizens including those residing in rural and remote areas may benefit from these 5G enabled IoT smart applications and services to create new economic activities and increase employment opportunities and thereby promote economic growth of the country?

&

Q.5. What initiatives are required to be taken by the Government to spread awareness among the citizens about IoT enabled smart applications? Should the private companies / startups developing these applications need to be engaged in this exercise through some incentivization schemes?

COAI Response:

1. The Internet of Things (IoT) is a paradigm that has been gaining traction in recent years, fuelled by the rapid advancements in communication technologies, particularly 5G. IoT technologies have the potential to transform various sectors and improve the quality of life of citizens.

2. However, despite the numerous benefits and potential applications of IoT technologies, there has been a digital divide that has been persistent in our country. The policy measures required to promote use of IoT technology and its infrastructure in rural areas are as follows:

   a. There is a need to create awareness among citizens about the benefits of IoT enabled smart applications and use cases in various industry verticals to ensure its adoption at large scale.

   b. There is a grave need to create specialized IoT training programs and partnerships with educational institutions to build a skilled workforce.

[5] https://courses.mooc.fi/org/uh-cs/courses/5g-mooc

c. It is also important to fund Research & Development projects focused on creating IoT solutions for rural challenges.

d. It is important to note that Innovation hubs can serve as centers for developing and testing IoT solutions tailored to local needs, fostering technological advancement in rural areas. Innovation hubs could also facilitate partnerships between local governments, educational institutions, and private companies along with supporting incubation services, technical support, and funding for IoT startups focusing on rural challenges. **Germany's Digital Hub** Initiative promotes digital innovation across various regions, with a focus on different technological sectors[6].

e. Startups are often at the forefront of IoT innovation. Financial incentives can stimulate growth and development of new IoT solutions & encourage local IoT solution development. Offer tax breaks, grants, and subsidized loans for IoT startups. Create competitive funding opportunities for IoT projects with societal impact. The **European Union's Horizon 2020** program offered funding for research and innovation projects, including several IoT. It has been a highly successful program with broad impact across Industries.

f. The high cost of IoT devices can be a barrier to adoption, especially for small businesses and consumers in rural areas. Implement schemes to reduce the cost of IoT devices for small and medium-sized enterprises (SMEs) and agricultural applications. Provide rebates or vouchers for IoT home devices to encourage consumer adoption. **Japan's Society 5.0** initiative includes subsidies for IoT adoption in various sectors, including agriculture.[7]

g. One of the most important example of this case is the India's 5G Lab of Center of Excellence which stands as a beacon of technological progress and innovation, showcasing the country's commitment to embracing and advancing cutting-edge technologies. This state-of-the-art facility symbolizes not only India's prowess in the field of telecommunications but also its dedication to fostering a digital ecosystem that is at par with global standards. The lab serves as a crucial platform for research, development, and testing of 5G applications and solutions, enabling India to carve a niche in the global 5G landscape.

3. There is a need to create awareness among citizens about the benefits of IoT enabled smart applications and use cases in various industry verticals to ensure its adoption at large scale.

   a. By deploying a multifaceted approach that involves educational initiatives, public demonstrations, and strategic partnerships, the government can play a pivotal role in raising awareness about IoT enabled smart applications.

[6] https://www.de-hub.de/en/

[7] https://www8.cao.go.jp/cstp/english/society5_0/index.html

b. Furthermore, incentivizing the private sector to contribute to this educational drive can catalyze the development and adoption of IoT technologies.

c. The combined efforts of public and private entities are crucial for realizing the vision of a smarter, more connected society that leverages IoT for economic growth, sustainability, and improved quality of life.

d. The initiatives that are required to be taken by the Government to spread awareness among the citizens about IoT enabled smart applications are as follows:

i. Develop educational campaigns that aim to inform the public about the practical benefits of IoT enabled smart applications, using various media channels including TV, radio, online platforms, and community events.

ii. Set up public demonstrations of IoT applications in action, such as smart street lighting in city centers or precision agriculture technologies in rural areas.

iii. Host national and regional IoT fairs and expos that bring together innovators, industry leaders, and the public to see the potential of IoT technology first-hand.

iv. Initiate targeted programs to demonstrate and educate about the benefits of IoT in rural and remote areas, addressing the specific challenges faced by these communities.

v. **Incentivizing for Developing relevant IoT Applications**: IoT applications tailored to specific regional needs can be more effective in demonstrating the practical benefits of IoT. Offer tax incentives or grants to TSPs that develop IoT solutions addressing local challenges. Facilitate public-private partnerships for community-specific IoT projects. In Singapore, the government collaborates with private companies to develop smart city solutions, a model that can be adapted for rural IoT applications[8].

vi. **Collaborating with Educational Institutions:** Educational institutions can play a crucial role in disseminating knowledge about IoT technologies. Integrate IoT-related subjects and practical projects into school and college curricula. Organize workshops and seminars in collaboration with tech companies and experts. The MIT Media Lab runs various programs and workshops on emerging technologies like IoT, serving as a model for educational collaboration.[9]

vii. **Policy Framework for IoT Integration in Government Services**: Integrating IoT into government services can improve their efficiency and accessibility, serving as a powerful example of IoT's benefits. Develop government programs that utilize IoT for

[8] https://www.smartnation.gov.sg/

[9] https://www.media.mit.edu/

public services like waste management, water quality monitoring, etc. Publicize successful implementations to increase public trust in IoT technology. **Barcelona's Smart City** project utilizes IoT for various urban services, demonstrating effective public-sector IoT integration[10].

4. Further, it is important to note that IoT or M2M communication have been here for a while and many regulatory policies have been developed to streamline the operations and foster innovation in this field. The industry has also represented the Government, many times, to address the restrictive features of the regulations governing these services to increase their adaptability. Some of these are elaborated under as follows:

A. Review of requirements of maximum number of Public IP addresses for data communications

1. The M2M communication related instructions dated 30.05.2019, mandate that Data communication for M2M SIMs can be allowed only to 4 predefined public URLs/ IPs. However, **we submit that this restriction is not in consonance with market realities. This restriction is proving to be a major issue with most popular M2M solutions. This restriction is also against the international precedents in countries making rapid advances in M2M communications like USA.**

2. Further, most M2M solutions are a result of collaborative efforts between multiple entities handling different legs of the M2M solution, **leading to a situation where the restriction of 4 IPs effectively constrains the innovations and effective M2M solutions and needs to be reconsidered.** A few use cases and applicable M2M solution are detailed below to illustrate the concern.

   a. **Vehicle tracking solutions / On-board diagnostic (OBD) solutions for vehicles:** Typically, these solutions are based on (a) Google Maps for location tracking and triangulation and (b) live streaming with the help of dashboard cameras for live video feed of the vehicle, and device analytics to check the health parameters of the vehicle. All related information captured from the M2M SIM is required to be sent to multiple third-party applications/entities collaborating in the M2M solution, which is much more than the limit of 4 Ips.

   b. **Connected cars**: Automobile companies offer access to real-time connectivity and infotainment in the form of live streaming and other OTT content, in addition to telematics, leading to requirement of more than 4 whitelisted IPs.

   c. **Point of Sale (PoS):** The modern-day POS machines provide multiple services like payments via all types of digital modes, recharges, e-payments like traffic challans etc.

[10] https://www.barcelona.cat/infobarcelona/en/tema/smart-city/boosting-barcelona-as-a-euro-mediterranean-capital_1275194.html

and connecting with GST application among other activities from a single interface device, making the 4 IP restriction completely unviable.

3. In view of the above, there is an urgent need to review the current restriction on data connectivity in line with market requirements. Therefore, these restrictive features may be analysed comprehensively taking into account service need aspects without sacrificing essential security consideration. Considering global nature of these services, the best international practices may also be studied to come up with the comprehensive solution.

B. Standardization/certification of IoT/M2M device

4. In order to ensure uniform growth of M2M devices, there is a need for **Device Standardization and Interoperability/testing standards for connectivity with MNO networks with appropriate certification to ensure no compatibility or interoperability issues. The voluntary One M2M standards by TEC are already in place and Government should encourage the OEMs to adopt these standards.**

5. Such standardization will address the on-going issues of overloading of mobile network signaling due to multiple PDP sessions by non-standard imported M2M devices with eSIM. The standardization will ensure network integrity and will be an important network security measure.

6. Further, in continuation of TEC Security guidelines for Consumer IoT devices, similar guidelines should also be issued for Enterprise IoT/M2M devices. **It might also be worth analyzing that a procedure akin to MTCTE certification of IOT devices prior to sale in market will enhance network security in the country.**

C. Integration of Foreign Subscription Manager Secure Routing (SM-SR) with Indian TSPs' network

7. We have already provided our detail submission on this issue vide our comments to the consultation paper on "Embedded SIM for M2M Communications" dated 25th July 2022. We submit that there is a need for uniform policy **for integration of Subscription Manager Secure Routing (SM-SR) platform for all the M2M devices being imported in the country.** Currently many devices being imported are equipped with eSIM with a bootstrap profile which is registered on company's own SM-SR platform based out of India. **Therefore, for facilitating download of Indian TSP's profile into these eSIM, SM-SR change is required through integration between these two SM-SR as per GSMA guidelines.**

8. Based on Authority's previous recommendations dated 5th September 2017, we understand that foreign IP integration between the donor SM-SR (hosted outside India) and the recipient SM-SR (hosted inside India) is allowed for swapping in line with the GSMA process requirement. **However, a clarity of policy is required in this aspect.**

9. We request the Authority to **consult and enunciate a clear policy that will simultaneously address the requirements of global interoperability and national security. We understand that one approach can be to ensure that while SM-DP remains within India, the SM-SR is allowed across the geographical boundaries to cater various use case requirements.**

10. Under this solution, **SM-SR can be owned by any party and can be located outside India as long as it is GSMA certified site, however, local MNO profile should be downloaded into the eSIM by local MNO SM-DP integration with foreign MNO SM-SR.** GSMA certification will also ensure the possibility of a reciprocal arrangement for Indian manufactured devices. If SM-SR has to be hosted in India, then SMSR swap within one year of timeline should be mandated after activating eSIM which are imported from outside India.

11. **Further, eSIM personalisation or remote provisioning should be carried out through the systems and facilities duly certified by SAS of GSMA. The SM-DP, SM-DP+ used for eUICC personalisation should be located within the geographical boundaries of India. The SM-SR, SM-DS and remote OTA platform should also be preferably hosted in India.**

12. Furthermore, SM-DS doesn't store MNO profile but stores EID, ICCID temporarily to redirect to MNO SM-DP+ platform. Hence SM-DS should not be mandated for GSMA SAS certification. **As SM-DS doesn't hold any profile data but only pointer towards to respective MNO system and it can be operated by private player who may not go for GSMA certification of SMDS as its used for their own devices ecosystem hence SAS certification should be preferred but not made mandatory.**

13. Accordingly, in view of the above, **we request for a non-obtrusive policy with a mandate to keep the SM-DP within India, while SM-SR, SM-DS can be located across the geographical boundaries to cater various use case requirements. Integration of India SM-SR and SM-DP to non-India SM-SR and SM-DP should be allowed. GSMA certification for SM-DS should be optional.**

D. Exemption for M2M SIMs from Data barring orders

14. The Authority is aware of the **import of M2M for Industry 4.0 and the national aspirations of leadership under Industry 4.0 therefore it is imperative that facilitative policies are implemented to ensure continued and non-disruptive service to M2M SIMs.**

15. We submit that is as IoT/M2M applications cover critical areas such as manufacturing, telemedicine & healthcare, connected vehicles, home equipment, smart meters etc., these should not be covered under the data services shut down orders issued by the Government authorities. **It is pertinent that as these SIMs comply with restrictive**

communication requirements, they cannot be used for any anti-social activities and can easily be excluded for data services shutdown requirements.

E. Non applicability of Tele verification / periodic verification requirements for M2M SIMs.

16. We submit that enterprise and non-P2P usage with restricted communication abilities of **M2M SIMs implies that tele-verification requirements, which are essentially for bona-fide personal use are not relevant in this scenario.** Also, these services do not have any person as an end user, and the present requirement of 6 monthly periodic verification in case of bulk mobile connection do not have relevance in case of M2M SIMs. Therefore, we request that the requirement of tele-verification prior to SIM activation and periodic verification as mentioned in the instructions dated 09.08.2012 shall not be applicable in case of M2M SIMs issued for M2M communication services.

F. Permit availability of eSIM from outside India

17. We submit that with the advances in technology, eSIM are becoming increasingly popular with much adaption in M2M devices. **We request that the Authority to facilitate easy import of eSIM produced outside, a measure that will also facilitate import of vehicles /devices from global manufacturer.**

G. Integrated SIMs

18. The **integrated SIM (ISIM) technology is very cost-effective and a boon for low power M2M devices that have multiple usage, especially in remote areas.** ISIM personalization should be allowed from outside India as this implementation is tightly integrated with modem chipset. Integrated SIM will follow the structure and security guidelines as issued by 3GPP and GSMA respectively - this should be introduced with proper DoT & GSMA guidelines.

H. Regulations on Custodian update in case of ownership change

19. We submit that M2M devices are deployed for various purpose such as street lighting, smart parking etc. where end custodian cannot be assigned. **We are seeing challenge in having this data added and updated periodically. Therefore, it is requested to issue facilitating guidelines to address this concern.**

Q.6. Industry 4.0 encompasses Artificial intelligence, Robotics, Big data, and the Internet of things and set to change the nature of jobs.

a. **What measures would you suggest for upskilling the top management and owners of industries?**
b. **What measures would you suggest for upskilling the workforce of industries?**

c. **What kind of public private partnership models can be adopted for this upskilling task? Please reply with proper justification and reasons and also by referring to the global best practices in this regard.**

COAI Response:

1. Industry 4.0 represents the fourth industrial revolution, characterized by a fusion of technologies blurring the lines between the physical, digital, and biological spheres. It integrates artificial intelligence (AI), robotics, big data, and the Internet of Things (IoT) to create interconnected and intelligent systems. Certain measures for upskilling the top management and owners of industries are as follows:

a. Executive Education Programs: Encourage participation in executive education programs focusing on digital leadership and transformation offered by leading business schools. These programs are tailored to help senior leaders understand and leverage Industry 4.0 technologies.

b. Online Learning Platforms: Use online platforms that offer courses created by top universities and companies on AI, IoT, and data analytics.

c. Cross-Industry Learning: Create opportunities for top management to engage in learning tours or exchanges with companies that are at the forefront of Industry 4.0. This can foster new insights and partnerships.

d. Strategic Advisor Engagement: Engage with digital transformation consultants or advisors who can provide personalized training and strategic insights to top-level decision-makers.

e. Leadership Retreats and Workshops: Host retreats focused on strategic thinking about the impact of Industry 4.0, featuring experts and thought leaders in the field.

f. Technical Training Programs: Implement technical training for specific tools and technologies that are becoming standard in Industry 4.0, such as advanced robotics, AI, and IoT platforms.

g. Digital Literacy Initiatives: Launch digital literacy initiatives to ensure all employees have basic knowledge of digital tools and platforms, which is fundamental in an increasingly automated workplace.

h. Collaborative Learning Environments: Foster collaborative environments where workers from different departments can learn from each other, sharing expertise and insights.

i. Apprenticeship Programs: Partner with technical schools and community colleges to offer apprenticeship programs that combine education with hands-on experience in advanced manufacturing and IT.

j. Continuous Learning Culture: Create a culture that encourages continuous learning and offers incentives for employees who upskill, ensuring that the workforce remains agile and adaptable.

k. Conduct executive education programs focusing on digital transformation and Industry 4.0. Partner with leading business schools and tech firms to offer customized workshops. Stanford University offers executive education programs in digital business strategy that could serve as a model. Similar programs could be established with support from Indian academia & institutes like the IIMs & other management schools[11].

l. The workforce needs new skills to operate and thrive in an Industry 4.0 environment, such as data analytics, IoT management, and cybersecurity. Develop technical training programs in partnership with industry players. Offer online courses and certifications to make training accessible. Siemens' partnership with various educational institutions to provide digital skills training. Similar programs could be built with support from Indian / Global Tech companies[12]

m. Further, PPP models can leverage the strengths and resources of both the public and private sectors for effective skill development. Government can provide funding and policy support, while private entities offer technological expertise and training resources.Focus on creating sector-specific training centres. For eg, **SkillsFuture Singapore** is a PPP initiative aimed at lifelong learning and skills development[13]

2. The public private partnership models can be adopted for this upskilling task are as follows:

   a. **Infrastructure Sharing**: Encourage passive infrastructure sharing, which is well-established in India. The government should allow the pass-through of infrastructure-sharing charges to promote active collaboration between Telecom Service Providers (TSPs) and other stakeholders.

   b. **Digital Literacy Initiatives**: Leverage existing government initiatives like the National Digital Literacy Mission (NDLM) and PM E-Vidhya. These initiatives, which span diverse sectors, can be enhanced through public-private partnerships to address critical issues and promote economic and social development.

[11] https://www.gsb.stanford.edu/exec-ed/programs/innovative-technology-leader

[12] https://www.siemens.com/global/en/company/sustainability/education/sce.html

[13] https://www.skillsfuture.gov.sg/

c. **Local Content and Training Collaboration**: Combine efforts of the public and private sectors to create localised digital content and training facilities, especially in rural and remote areas. This would help in bridging the digital divide and enhancing digital literacy at the grassroots level

Q.7. What are the policy, regulatory and other challenges faced by MSMEs in adoption of Industry 4.0. Kindly suggest measures to address these challenges. Provide detailed justification with reasons along with the best practices in other countries.

COAI Response:

1. Micro, small, and medium enterprises (MSMEs) play a pivotal role in the growth of manufacturing sector in a nation's economy. MSMEs are considered the pillars of Indian economy due to their considerable contribution to GDP, exports and employment generation.

2. Various studies have indicated that there are many challenges that MSMEs are facing to embrace Industry 4.0. The major challenges are:

Policy Challenges:

a. Limited access to finance: MSMEs often struggle to secure adequate funding for capital-intensive Industry 4.0 upgrades. High-interest rates and cumbersome loan processes further hinder their ability to invest.

b. Lack of awareness and knowledge: Many MSMEs lack awareness about Industry 4.0 technologies and their potential benefits. Limited understanding of implementation complexities and return on investment deters them from adopting these solutions.

c. Skill gap: Implementing Industry 4.0 requires a skilled workforce to operate and maintain advanced machinery and systems. The current skillsets in many MSMEs are not aligned with these demands.

d. Fragmented policy landscape: Inconsistent and overlapping policies across different government agencies create confusion and hinder streamlined implementation of Industry 4.0 initiatives, coordination between various ministries, Industry verticals, TSPs for different use cases.

Regulatory Challenges:

a. Data privacy and security concerns: MSMEs grapple with complex data privacy regulations and lack the resources to implement robust cybersecurity measures, hindering their ability to leverage data-driven technologies like AI and analytics.

b. Evolving regulatory environment: The rapid pace of technological advancements makes it challenging for MSMEs to keep up with changing regulations, leading to compliance issues and uncertainty.

Other Challenges:

a. Resistance to change: Traditional mindsets and fear of disruption can make MSMEs hesitant to embrace new technologies and adapt their business models.

b. Lack of economies of scale: Many MSMEs operate in silos, hindering their ability to negotiate better deals with technology vendors and access resources like advanced training at affordable costs.

3. **Measures to Address the Challenges:**

a. Subsidies and tax breaks: Providing financial incentives for MSMEs to invest in Industry 4.0 technologies and infrastructure can bridge the funding gap and encourage adoption.

b. Awareness and capacity building programs: Government and industry bodies can organize workshops, training programs, and knowledge-sharing platforms to educate MSMEs about Industry 4.0 benefits and implementation strategies.

c. Skill development initiatives: Public-private partnerships can establish vocational training programs focused on Industry 4.0 skills, including digital literacy, data analysis, and AI awareness, to equip the workforce for the future.

d. Digital infrastructure development: Prioritizing broadband connectivity, cloud infrastructure expansion, and digital literacy campaigns can create a level playing field for MSMEs across regions.

e. Streamlined regulatory framework: Consolidating policies, simplifying compliance procedures, and offering regulatory sandboxes for pilot testing of innovative solutions can reduce uncertainty and encourage experimentation.

f. Data privacy and security support: Providing MSMEs with affordable data encryption tools, cybersecurity training, and clear data governance guidelines can address their concerns and enable secure data utilization.

g. Collaborative platforms: Establishing industry clusters and facilitating knowledge exchange between MSMEs and larger corporations can foster innovation and economies of scale.

4. Other challenges:

a. Fear of the likely resource pressures- finance, technology, human-talent, infrastructure, and new operational skill.

b. Fear of exorbitant cost of transitioning from the existing state to the new Industry 4.0 state of operation.

c. Potential concerns in Information technology related capabilities in terms of investment, operation, interoperability, cyber security, etc.

d. Fear of embracing this radical Industry 4.0 approach which is still to provide tangible and visible deliverables and has a risky return on investment.

e. Global Best Practices:

   i. Germany: Their "Mittelstand 4.0" initiative provides financial assistance, training programs, and a collaborative platform for MSMEs to adopt Industry 4.0 solutions.

   ii. South Korea: Their emphasis on open innovation, 5G infrastructure rollout, and regulatory sandboxes fosters a vibrant ecosystem for startups and MSMEs to experiment with Industry 4.0 solutions.

Q.8. What additional measures are required to strengthen the National Trust Centre (NTC) framework for complete security testing and certification of IoT devices (hardware as well as software) under DoT / TEC. What modifications in roles and responsibilities are required to make NTC more effective? Kindly provide your comments with justification in line with the global best practices.

COAI Response:

1. The Framework of National Trust Centre for M2M/IoT Devices and Applications was released by TEC in March 2022. According to these recommendations, it was also decided that for certification of software products related to M2M devices, STQC (Standardization Testing and Quality Certification) under MeitY may be the agency to carry out such testing. Whereas, testing and Certification of IoT devices hardware is already covered in Essential Requirements (ERs) under MTCTE having testing specifications related to EMC, Safety, communication interfaces, IP, SAR and Security. However, it is pertinent to note that no such specific trust centre for IoT devices appears to be functional under TEC or STQC and no specific IoT related security testing specifications have been published till date.

2. To strengthen the National Trust Centre (NTC) framework for complete security testing and certification of IoT devices in the context of the Department of Telecommunications (DoT) / Telecommunication Engineering Centre (TEC), several additional measures and modifications in roles and responsibilities can be considered:

   a. Develop and regularly update comprehensive security protocols and standards specifically tailored for IoT devices. This includes stringent encryption standards, secure communication protocols, and robust data privacy measures.

b. Establish a schedule for regular audits of IoT devices to ensure ongoing compliance with security standards.

c. Conduct regular training for the staff at NTC to keep them updated with the latest security trends and threats.

d. Launch awareness programs for manufacturers and users about the importance of IoT security.

e. Clearly define the roles and responsibilities within NTC for various aspects of IoT security, such as standard setting, certification, auditing, and enforcement.

f. Establish dedicated teams for different IoT sectors (like healthcare, automotive, home devices) due to the varied nature of these devices.

i. Introduce a role focused on continuous monitoring of the IoT threat landscape and updating the NTC framework accordingly.

3. By implementing these measures and redefining roles and responsibilities, the NTC can significantly enhance its effectiveness in ensuring the security of IoT devices, both in hardware and software aspects.

4. **Security obligations for the Telecom services being provided by unlicensed entities:**

a. There are currently companies operating with telecom ecosystem that are offering a variety of services (IoT & M2M services) using license exempt spectrum and are not subject to National security Sirective on Telecom sector (NSDTS) for critical infrastructure such as Water, Power, Gas etc.

b. These include data collecting, tracing, and tracking services using low-power, short-range radio frequency devices such as wireless sensors and actuators, smart metres, wireless industrial applications, wideband data transmission systems, location systems, wireless control systems, etc.

c. Antennas, wireless carriers, signalling protocols, as well as other network protocols, including IP, are required for the delivery of such services. These components are also necessary for the telecom operations carried out by licensed TSPs. Fundamentally, whether these services are offered by an unlicensed entity or a licensed TSP, the technology requirements for supplying them remain the same.

d. In this regard, we suggest that TRAI recommend NSCS and DoT to immediately finalize the decision on Critical Services in the M2M sector. Consequently, Smart Meters should come under critical M2M services and should allowed to be offer services using only the licensed spectrum band.

e. TRAI to further recommend making the procurement of devices and network equipment mandatory from only 'Trusted Sources' as defined under NSDTS directives where the unlicensed entities providing services akin to Telecommunication sector are also covered.

Q.9. IoT security challenges and requirements vary significantly across different industry verticals. Is there a need to develop sector-specific IoT security and privacy guidelines?

&

Q.10. If answer to Q.9 is yes, is there a need for a common framework and methodology for developing such sector-specific guidelines?

COAI Response

1. The development of sector specific IoT security and privacy guidelines, underpinned by a common framework, is essential to address the diverse and complex challenges posed by IoT across different industry sectors. By doing so, not only is the integrity and security of IoT systems upheld, but also their interoperability and compliance with broader regulatory standards are ensured. This dual approach allows for the tailored protection of sector-specific needs while maintaining a consistent security posture across the IoT landscape.

2. Further there is a need to develop sector-specific IoT security and privacy guidelines due to the varied challenges and requirements across different industry verticals. Industries like healthcare, automotive, manufacturing, and home automation all use IoT differently, resulting in unique vulnerabilities and security needs. The sector-specific guidelines would ensure that security measures are tailored to address these distinct risks effectively, enhancing overall cybersecurity resilience in each industry. The Health Insurance Portability and Accountability Act (HIPAA) in the U.S. provides specific guidelines for protecting sensitive patient data, a model that can be adapted for healthcare IoT[14].

   a. It is pertinent to note that there is a need for a common framework and methodology for developing these guidelines. This approach ensures consistency, interoperability, and comprehensive coverage of security aspects across different sectors.

   b. A common framework provides a standardized approach to security, ensuring that basic security principles are consistently applied across different sectors. This helps in maintaining a baseline of security practices that are universally recognized and adhered to.

[14] https://www.hhs.gov/hipaa/index.html

c. A common framework ensures interoperability and compatibility among devices from different sectors, reducing the risk of security breaches due to incompatibilities.

d. The framework can offer a structured methodology for risk assessment that is adaptable to different sectors. This includes identifying common threats and vulnerabilities, while also allowing for sector-specific risks to be addressed.

e. A common framework can be designed to be adaptable, allowing for the integration of emerging technologies and evolving threat landscapes. This makes it easier to update and evolve sector-specific guidelines as needed.

f. The Digital Personal Data Protection Act, 2023 (DPDP) provides a broad framework for data protection that can be adapted for specific sectors.

Q.11. Please suggest regulatory and policy interventions required to ensure privacy of the massive amount of sensitive user data generated by IoT applications specifically in light of the Digital Personal Data Protection Act, 2023. Kindly provide justifications along with the global best practices.

COAI Response

1. We submit that the Digital Personal Data Protection Act, 2023 adequately addresses the issues pertaining to privacy of sensitive user data generated by IoT applications and there is no need for any more regulatory and policy interventions at this time.

Q.12. What additional policy and regulatory measures are required to encourage research and development of IoT use cases in various sectors? Is there a need to incentivize startups for research and development of IoT enabled use cases in various industry verticals? If yes, kindly suggest measures for the same.
&
Q.13. What measures should be taken to encourage centres of excellence to handhold startups working in the development of use cases and How can the domestic and foreign investors be encouraged to invest for funding the startups for these kinds of development activities?

COAI Response

1. 5G needs to be capitalized for Industry 4.0 proliferation in the Country. Various Industry verticals wish to enhance their productivity, efficiency and have sustainable growth. Industry verticals are looking for such uses cases for their Operational requirements be it in IOT, CLOUD, Digital twin AR VR etc. To increase the research and development in these respective domains, collaboration needs to be emphasized between Industry, Academia, start-ups, and technology solution providers. 5G ecosystem players involved in such center of excellence needs to be incentivized. Industry vertical adopting the industry 4.0 initiative needs to be incentivized. Encouragement for Devices ecosystem

players with lower taxes & duties for few initial years will help in adoption of 5G and IOT applications in various industry verticals.

2. One of the most important examples of this case is the India's 5G Lab of Center of Excellence which stands as a beacon of technological progress and innovation, showcasing the country's commitment to embracing and advancing cutting-edge technologies. This state-of-the-art facility symbolizes not only India's prowess in the field of telecommunications but also its dedication to fostering a digital ecosystem that is at par with global standards. The lab serves as a crucial platform for research, development, and testing of 5G applications and solutions, enabling India to carve a niche in the global 5G landscape.

Q.14. Whether there is a need to make changes in relevant laws to handle various issues, including liability regime and effective mechanism for redressal and compensation in case of accidents, damages, or If yes, give detailed suggestions.

COAI Response

No Comment

Q.15. Is there a need to have a separate security mechanism for Multi-access Edge Computing (MEC)? If yes, please give your inputs and suggestions with regard to policies, rules, regulations and guidelines.

COAI Response

1. Establishing a comprehensive security mechanism for Multi-access Edge Computing is essential in the evolving landscape of 5G and IoT. It requires a blend of specialized security protocols, robust policy frameworks, and multi-stakeholder collaboration to address the unique security demands of edge computing. By adopting these measures, India can ensure the secure and resilient deployment of MEC, a critical component in the next generation of wireless technology infrastructure**.**

a. A specialized security mechanism is crucial to protect against threats like data breaches, unauthorized access, and cyber-attacks at the network edge.

Suggested Policy Interventions:

i. Develop security protocols tailored to the edge environment, considering the higher risk of physical access and the need for rapid data processing.

ii. Implement robust encryption and authentication measures to secure data transmission between edge devices and central networks**.**

International Best Practice:

The ETSI whitepaper on MEC security outlines various security considerations and recommendations[15].

b. **Policy, Rules, and Regulation Suggestions for MEC Security:** Establishing clear policies, rules, and regulations is vital to standardize and enforce security practices across MEC implementations.

Policy Interventions:

i. Define compliance standards for MEC providers, including requirements for regular security audits and vulnerability assessments.

ii. Set guidelines for data localization and processing at the edge, keeping in mind privacy laws and regulations.

International Best Practice:

The European Telecommunications Standards Institute (ETSI) has developed standards for MEC that include security aspects.[16]

c. **Collaboration with Industry and International Bodies:** Collaborating with industry stakeholders and international bodies ensures that MEC security mechanisms are up-to-date with global standards and best practices.

Policy Interventions:

i. Engage in partnerships with tech companies and cybersecurity experts to share knowledge and resources.

.

ii. Actively participate in international forums to align MEC security standards with global norms.

Q.16. What are the policy measures required to create awareness and promote use of Metaverse, so that the citizens including those residing in rural and remote areas may benefit from the Metaverse use cases and services to create new economic activities and increase employment opportunities and thereby promote economic growth of the country?

COAI Response:

1. Generating awareness and conceptualising application of core technologies of metaverse (viz. augmented reality, virtual reality and mixed reality) for the larger public good are likely to lead to more diverse and widespread adoption, as well as greater opportunities to drive

[15]

[16] https://www.etsi.org/technologies/multi-access-edge-computing

innovation. Policymakers should leverage the resources of industry participants and civil society in its efforts to generate awareness, build capacity, and ensure democratic access to the metaverse.

2. **Certain key policy measures may be considered in this regard:**

a. *Awareness and Accessibility*: Given that the metaverse is still at a nascent stage of development and adoption, it is unknown to a large section of the population. The growth of the metaverse should be accompanied by efforts to educate companies, consumers, and policymakers. The government, through collaborations and partnerships with industry, think tanks, academia, civil society organisations, should fund, facilitate and raise in awareness through campaigns and exhibitions to demonstrate best practices within the industry and to make the public aware of new and existing use cases, how to use the metaverse, and how it may benefit them, and how to protect themselves from potential harms. Industry leaders in other sectors (particularly, non-digital sectors) must also be made aware of the potential of metaverse applications, to enable widespread adoption.

A diverse and relevant set of use cases is a sure shot way to promote access and awareness – especially with India’s young population – and India’s experiments with Unified Payment Interface and Digital Public Infrastructure initiatives are a clear indicator of this. Metaverse products and virtual worlds must also account for the diverse linguistic, cultural, and socio-economic backgrounds of the citizens of Bharat. Catering to rural and semi-urban populations in particular is critical to ensure that they are encouraged to access and use services that may be provided to them through the metaverse. Large technology companies (with their advanced technology capabilities) in collaboration with SMEs and start-ups (with their knowledge of local contexts) will play a crucial role in developing metaverse use cases for Bharat to ensure that such diverse needs are met. Investment in developing talent and incubating new use cases is also critical in this regard, and policymakers can consider creating a dedicated fund for metaverse use cases which cater to rural populations or other unserved communities.

Accessibility doesn’t just mean access to the technology. It also means providing opportunities and solutions for people with disabilities. There are already a suite of applications that are benefiting people with disabilities, including speech to text, and hand and eye tracking. These are a few examples of applications that make the technology more approachable and beneficial for those with disabilities.

b. *Skilling for the metaverse*: Increasing innovation in the metaverse must also be accompanied by upskilling of the Indian workforce to be able to meaningfully participate in the growth of the industry. There exists significant opportunities for large-scale employment, given the advent of new job profiles such as metaverse architects, virtual event planners, AR/VR Software Engineers, and more.

Initiatives must be introduced to create readiness for a metaverse-centric technology landscape, which would prepare the individuals for the complexities as well as the advantages metaverse brings with itself. One of the most effective ways to build readiness for emerging technologies essential for metaverse is to revise the present educational curriculum (both at school and college level) to ensure that it is updated to meet the needs of emerging technologies like AR, VR,MR and Artificial Intelligence. This could include introducing internship and skill-development programmes at the school and college level. As part of these programmes, students can gain the necessary hands-on experience and practical learning to improve their employability and industry readiness.

Besides changes in curricula and skill development programmes, there is a need to create awareness about the future of jobs in educational institutions. Opportunities in XR technologies should be brought to the notice of parents and students to promote greater uptake of such career paths. The focus should be to design jobs and career pathways based on skills and experience, and not educational degrees.

Given that a large number of reputable educational institutions in India are funded and operated by government bodies, India has the opportunity to introduce a strong future-led, innovation-focused curriculum. Policymakers can also take the lead in facilitating collaboration between educational institutions and industry players to assess the existing skills gap and co-design roadmaps to adapt existing programs and strengthen industry-university cooperation. Several companies have already begun investing in programs to skill students and educators in new technologies, as well as to upskill those presently engaged in allied industries, such as investing in creators to help them develop skills in AR, VR and immersive media. Existing programs for upskilling and reskilling in emerging technologies should be strengthened and expanded with increasing industry participation.

c. *Integration with existing systems*: Significant value can be derived from the application of the metaverse in existing digital and physical ecosystems. Policymakers and implementing entities/agencies should work with industry stakeholders and developers to determine how best to integrate these technologies into existing IT systems. Through a combination of private sector expertise in metaverse deployment and the mandate of the public sector to ensure service delivery to the last-mile, the metaverse can play an increasingly critical role in the lives of Indians living in remote and rural areas. Some examples of use cases for potential collaboration have been indicated below:

d. Training: The ability to conduct remote skilling through the metaverse eliminates the need for citizens in more rural areas to travel to larger cities to receive training, and also requires less infrastructure (physical space, equipment). With India expected to have 1 billion smartphone users by the end of 2026, enabling citizens to access such online spaces through their smartphones would additionally catalyse such programs.

To enable such use cases, policymakers should consider integrating metaverse technology developed by the industry into existing skill development programs.

i. E-governance: Citizen services can be provided remotely through the metaverse, enabling rural citizens to access a plethora of services which may be currently difficult to access. Physical requirements of document submission, in-person verification and inspection to avail government services or benefits can be eliminated through the metaverse.

ii. Tourism: Through the virtual world, it's possible for tourists to explore a destination before they arrive. Tourism departments and district officials in India can utilize metaverse tourism to be able to market and brand rural destinations for tourists, providing a boost to the local economy.

e. Adoption of XR in government applications to promote innovation and affordability

i. XR technologies have the potential to revolutionize the operation of government agencies, improve decision making, and enhance delivery of public services. Notable use cases include transformation of citizen engagement, training at scale, enhancement of urban planning and promotion of tourism.

ii. As government agencies in India increase investment in XR infrastructure and R&D, it will make technologies affordable, attract companies, foster entrepreneurship, and support the growth of XR-related industries in India. For instance, promoting the use of XR in skilling, tourism, education and training, will help expand the demand for these technologies.

iii. It is imperative that all Indian government departments stay at the forefront of technological advancements and contribute to the creation of a thriving XR ecosystem.

f. *Access to digital infrastructure*

i. *High-speed Internet:* The most important part of setting up a metaverse friendly technological infrastructure is to ensure easy access to high-speed internet. High speed internet as a foundational component can be achieved by investing and focusing on building necessary network frameworks which support 5G, while supporting hotspot as public access points for the population's wide use. Recently, the government introduced a high-speed internet project focusing on 6.4 lakh villages in India under the BharatNet initiative, with an aim to provide seamless connectivity to the rural areas. While the program is in its initial stages, and the government seeks to expand it to the national level, we recommend integrating 5G technology as well as collaborating with telecom players in order to make the implementation of this initiative more effective.

ii. *Community Centres:* Since in rural areas the general community at an individual level will not have the financial wherewithal to seek access to the digital infrastructure and hardware required to access the metaverse, the government can encourage setting up of digital infrastructure in the form of community centres, which are open for everyone's access. Setting up community centres equipped with high-speed internet, computers with adequate specifications can help bridge the digital divide and metaverse supporting hardware like AR/VR headsets. These centres can serve as hubs for digital literacy training, metaverse awareness programs, and skill development workshops. The educational institutions in rural areas, i.e., K-12 schools as well as colleges and universities can be used as centres to run workshops and educational programs using the metaverse. Such workshops and programs can be on varied topics, and the awareness regarding metaverse. Additionally, technological workshops may be conducted with a focus on metaverse, which also impart knowledge about the various use cases of various metaverse tools in different industries as well as privacy and security risk mitigation measures.

g. *Ease* entry barriers for hardware import and incentivize manufacturing in India

i. Lack of affordable hardware in India impacts the ability of the Indian ecosystem to reap the benefits of the metaverse economy and underlying futuristic technologies. Many companies are working to make XR devices more affordable over time, but there are several things the government could consider to do now that would have an immediate effect on the price of devices, including lowering tariffs.

ii. Easing out the requirement of multiple certifications for selling devices in India could be explored. Presently, testing and certification for telecom and related IT equipment is broadly under the purview of several agencies across different ministries. These include the Bureau of Indian Standards and the Telecommunication Engineering Centre, which administers the Mandatory Testing and Certificate of Telecom Equipment (MTCTE) requirements. Due to this complex administrative structure, it is likely that certain types of devices like VR/AR devices would have to adhere to multiple standards, testing and certification requirements. Harmonizing the testing and certification functions will ensure that the overlaps between different administrative agencies is limited. Further, implementation of regulatory sandboxes collaboratively between various regulators can also be one of the ways in addressing entry barriers for specific use cases.

iii. Additionally, inclusion of XR technology and related products in the Production Linked Incentive (PLI) scheme and other incentives in the form of tax benefits to attract XR related hardware manufacturers to the country can also be considered.

Q.17. Whether there is a need to develop a regulatory framework for the responsible development and use of Metaverse? If yes, kindly suggest how this framework will address the following issues:

i. **How can users control their personal information and identity in the metaverse?**
ii. **How can users protect themselves from cyberattacks, harassment and manipulation in the metaverse?**
iii. **How can users trust the content and services they access in the metaverse?**
iv. **How can data privacy and security be ensured in the metaverse, avatars across different platforms and jurisdictions?**

COAI Response

1. Regulation often lags technological developments. One way to make regulation future proof is to make it technology agnostic. Technologies like the metaverse are at a very early stage of development. In many cases, the metaverse looks to model the real world, and as such may see the similar interactions, transactions and activities that we see in the real world. In this context, it is important to view the metaverse within the existing regulatory framework first, to assess whether regulations that govern real world actions would be effective in regulating similar actions carried out in the metaverse. The metaverse does not exist in a regulatory vacuum, with several technology neutrality laws in the current Indian legislative and regulatory framework which adequately address issues in connection with the metaverse or relating to the development and use of metaverse.

   We therefore do not see any requirement for the development of a regulatory framework to specifically govern the responsible development and use of metaverse. This is an approach being considered in various other global jurisdictions. Most countries are not looking to introduce metaverse-specific legal-framework, with jurisdictions like the EU reporting that its existing legal framework is robust and future-oriented enough to apply to several aspects of the development of virtual worlds. In addition to legislation, voluntary codes and standards set by global industry alliances are also effective in regulating the metaverse. The indicative list below demonstrates the adequacy of existing laws, regulations, standards, and guidelines that govern the development and use of metaverse.

   a. **Control over personal information:** The new data protection regime proposed to come into force in India (i.e., the Digital Personal Data Protection Act, 2023 (**DPDP Act**)) is a comprehensive and robust regulation, which introduces various mechanisms to provide users with autonomy over their personal data. As such, users will now have greater control over the data they share with entities to sign up to the metaverse, as well as any personal data they may share during the course of their use of the metaverse. The DPDP Act provides users with various rights including the right to access and right to correction and erasure in connection with their personal data which would enable users in the metaverse to assert control over how their personal information and various identities are featured in the metaverse. For instance, **the principles outlined in the DPDP Act should be applied to metaverse as well.**

b. **User Safety and trust**: Various acts that may jeopardise user safety are regulated under criminal laws. For instance, the Indian Penal Code, 1860 (IPC) penalises the distribution and circulation of obscene material, defamatory content or content that causes disharmony or feelings of enmity or hatred or ill-will between specific groups of members. This serves to strengthen metaverse users' trust in the content they access within metaverse. The IPC further penalises theft, dishonest and fraudulent concealment and destruction of property which would equally apply to online activities. Various laws on content moderation also serve to protect users in the metaverse, as further described in our response to Question 21. Additionally, the Indian Computer Emergency Response Team has also been set up to prevent, forecast and coordinate responses to a variety of cyber incidents which may affect user safety online.

With respect to children's safety, the (Indian) Protection of Children from Sexual Offences (POCSO) Act, 2012 prescribes punishment for the use of a child in pornographic material, thereby ensuring that the content accessible in the metaverse is not obscene. Information technology laws also specifically prohibit the handling of any sexually explicit electronic material relating to children. Similarly, the DPDP Act imposes certain restrictions on entities that process children's data such as prohibiting them from undertaking any processing that is likely to have a detrimental effect on the well-being of a child and tracking, monitoring the behaviour of, or directing targeted advertisements at children. These regulations ensure that the content and services that children may access in the metaverse are strictly regulated. Recommendations issued by international agencies are also relevant and can act as voluntary guidance for operating entities. For instance, the United Nations Children's Fund has listed various recommendations in its rapid analysis report titled '*The Metaverse, Extended Reality and Children*'.

The (Indian) Consumer Protection Act, 2019 (CPA) governs the marketing, sale and purchase of goods and services in India in order to safeguard the interest of consumers. A specialized central authority created under the CPA is empowered to regulate illegal conduct and consumer harm including certain unfair trade practices such as making false representations about the standard, quality, characteristics, uses or benefits of services, giving warranties/guarantees that are misleading etc. Such provisions under law would ensure users in the metaverse are protected against any deficient digital services and any technical issues with digital assets.

While, the proposed Digital India Bill, will outline a regulatory framework to enable and safeguard the development of emerging technologies and address the consequent risks, following are some of the measures recommended by various experts and studies:

i. To ensure mental safety, features which allow users to block, mute, and report violations are the baseline tools which should be incorporated in the technologies built for accessing Metaverse. Additionally, there would be requirements for ensuring the report of abuse, blocking certain users, setting virtual buffers, and placing appropriate privacy controls.

ii. Features such as personal boundary which enables creation of distances when interacting in VR is one of critical features to provide users more control and address safety issues.

iii. To ensure physical safety of users, wearables could enable creation of a pre-established boundary or space in which the user can move once a headset is on. To address ergonomics of the wearables and ensure user comfort investment R&D is needed to re-design the technology.

iv. Developers should regularly update their XR products and standards for using them with physical and mental safety in mind.

v. Safeguarding vulnerable data via encryption, auto deleting data that is no longer needed are some of the ways to ensure security of the data.

c. **System Security:** The DPDP Act requires entities that handle personal data to implement technical and organisational measures and take reasonable security measures to prevent personal data breaches.. International cybersecurity standards can also be relied upon to determine what security measures should be adopted in the metaverse. For instance, the National Institute of Standards and Technology (NIST) released standards designed for organizations to manage their privacy and cybersecurity risks, which ensures security-by-design in metaverse development.

2. We recognise that the metaverse is a new technology and may therefore give rise to unforeseen risks as it continues to develop, and as new use cases are discovered. It is proposed that such risks be assessed and addressed on a case-by-case basis through a multi-stakeholder approach, with participation from policymakers, public agencies, industry, developers, academia, consumers and civil society. This may take the form of consultations, which are already extensively carried out by various regulators in India to seek public opinion on upcoming regulatory issues.

3. Globally, similar programs like the Metaverse Initiative at the World Economic Forum have been introduced, which brings together over 150 partners across industries and geographies from the private sector, civil society, academia and policy (such as Sony, Stanford University, Meta, Interpol, Deutsch Bank, United Nations Office of Counter Terrorism, the Singapore Government etc.,) to define the parameters of an economically viable, interoperable, safe and inclusive Metaverse.

4. The EU has decided not to develop Metaverse-specific regulation for the moment, deeming that the current legislative framework is robust and future-oriented, with the Digital Services Act, Digital Markets Act, Data Governance Act, Data Act and General Data Protection Regulation.

5. In its draft report[17] Virtual worlds: opportunities, risks and policy implications for the Single Market, the European Parliament "Welcomes the Commission's commitment to monitor the development of virtual worlds; invites the Commission to draft a report on this subject every two years and to transmit it to Parliament and the Council; asks the Commission to pay attention to the potential emergence of problems in the Web 4.0 that already exist in the Web 3.0, such as the proliferation of fake news, infringement of intellectual property rights, cyberterrorism, sexual abuse of minors and cyberbullying, among others"

Q.18.Whether there is a need to establish experimental campuses where startups, innovators, and researchers can collaborate and develop or demonstrate technological capabilities, innovative use cases, and operational models for Metaverse? How can the present CoEs be strengthened for this purpose? Justify your response with rationale and suitable best practices, if any.

COAI Response

1. Jurisdictions globally are looking to regulatory sandboxes to support metaverse innovation. For instance, the EU plans to promote the use of virtual worlds regulatory sandboxes by its Member States. Reports commissioned by the South Korean government also recommend creating regulatory sandboxes to test metaverse applications in games. The Innovation License introduced by the Bahraini Telecommunications Regulatory Authority also encourages development and deployment through testing and trial of new wireless technologies and services. In India, the Government of Telangana has set up a regulatory sandbox for Web 3.0 for innovation in various fields including metaverse. It is recommended that more such initiatives be encouraged and introduced to enable active industry participation in the growth of this industry.

2. Centres of Excellence (CoEs) are perfectly positioned to facilitate these ecosystems in India, as they serve as a platform to bring together the public and private sector to drive co-creation, problem-solving, nurturing innovation and disseminating best practices. We note that some public-private partnerships have been announced towards the creation of CoEs for metaverse in India, such as the International Hub for Education in Mixed Reality by the Karnataka Digital Economy Mission, Excelsoft Technologies, Mysuru and UNESCO Mahatma Gandhi Institute of Education for Peace and Sustainable Development. At a global level, KPMG is set to establish its Centre of Excellence for Metaverse and digital twins in Saudi Arabia.

[17] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2022/2198(INI)

3. Policymakers may strengthen CoEs for the metaverse by promoting their creation and increasing investments in such initiatives. Regulators like the Securities and Exchange Board of India have developed an overarching framework and guidelines for how their regulatory sandboxes should function, and a similar approach may be adopted to streamline and strengthen the priorities, operations and functioning of CoEs. CoE can also be strengthened by enabling ongoing platforms for long-term dialogue and cooperation with industry stakeholders, to share knowledge and ensure a shared understanding of these technologies as they are developed. The introduction of accelerator programs within CoEs can also enable support for industry participants to build partnerships and access resources within the metaverse market. For instance, the Dubai International Financial Centre (DIFC) launched a Metaverse Accelerator Programme to support innovative metaverse start-ups by helping them explore partnerships, gain exposure to investors, access a regulatory sandbox and obtain marketing support. Similar programs should be set up in India. Further, the Singapore government (through its Personal Data Protection Commission) has collaborated with organisations like Open Loop to facilitate policy prototyping, which involves testing of policy measures within a controlled environment to inform the introduction of standards and guidelines for the industry. CoEs may consider exploring such collaborations.

4. Examples of international best practices[18]: In Europe, The Virtual and Augmented Reality Industrial Coalition is a platform for structured dialogue between the European VR/AR ecosystem and policymakers. It has produced policy recommendations and a roadmap for sector collaboration and support.

Q.19. How can India play a leading role in metaverse standardization work being done by ITU? What mechanism should be evolved in India for making an effective and significant contribution in Metaverse standardisation? Kindly provide elaborate justifications in support of your response.

COAI Response

1. The metaverse will reach its full potential only if built on a foundation of common technical standards and protocols empowering both businesses and people to seamlessly navigate and travel between multiple destinations and experiences, just like we can browse the internet today freely. The development of technical standards in specific areas is therefore crucial to a baseline level of interoperability that mirrors the kind of open internet protocols we see in place today, lowering barriers to entry and facilitating market access by small firms and developers.

2. While such standards may be set by government bodies and global alliances like ITU, given emerging technologies like metaverse are nascent, a global industry-wide cooperation on interoperable standards will be critical to build the metaverse which drives economic value for all participants and necessary to bring together companies and organizations that have

[18] https://digital-strategy.ec.europa.eu/en/policies/virtual-and-augmented-reality-coalition

a shared interest to develop, define, and evolve open standards that will drive a truly interoperable metaverse.

a. Given the potential of metaverse, Indian stakeholders including developers, experts, companies, startups, academia should look to actively participate and contribute to the global standard setting process. In this context, policymakers in India can consider the various measures to support, contribute and lead efforts towards the evolution of the global standard setting process.

i. *Support international, multi-stakeholder efforts to develop baseline technical standards on an evolving basis*: India has a strong and burgeoning community of developers and open-source innovators who are well-placed to contribute to the creation of global standards, at various standard setting bodies including at the ITU. Policymakers in India should enable, encourage and support these communities and other industry participants to engage in industry-led efforts and alliances, to ensure that domestic principles are accounted for and built into these standards.

ii. *Align domestic requirements with globally agreed standards:* To enable the streamlined and cohesive growth of the domestic Metaverse industry, India policymakers must ensure that any regulation, policy measure or initiative in relation to standards accounts for corresponding international multi-stakeholder efforts, to enable alignment with global best practices.

Q.20.(i) What should be the appropriate governance mechanism for the metaverse for balancing innovation, competition, diversity, and public interest? Kindly give your response with reasons along with global best practices.

COAI Response

1. As mentioned above in Question 19, there is no separate need for a regulatory framework to govern the development and use the metaverse as the metaverse does not exist in a regulatory vacuum. The current legislative framework goes a long way in effectively governing the industry and adequately addresses issues arising out of or in connection with the metaverse. Any contemplation of a fresh legislative framework to govern the metaverse could create regulatory uncertainty, arising from overlaps with existing laws.

Q.20.(ii) Whether there is a need of a national level mechanism to coordinate development of Metaverse standards and guidelines? Kindly give your response with reasons along with global best practices.

COAI Response

1. Policymakers may consider the creation of a central multi-stakeholder agency to coordinate and build a consensus on domestic priorities and interests in relation to

metaverse standards and guidelines. For instance, the Electronics and Information Technology Division council (LITDC) at the Bureau of Indian Standards, recently established a new panel on metaverse. The scope of the metaverse panel is as follows:

a. Mirror the work of ISO/IEC SEG 15 & finalize India's inputs on their documents along with attending their meetings.

b. Investigate the needs for standardization in the area of metaverse, taking into account current research, technology and standardization activities, and trends.

c. Recommend an initial roadmap for standardization activities in the area of metaverse.

d. Make further recommendations to LITDC as appropriate.

2. We recommend that TRAI, DoT along-with TSPs should work with BIS and such bodies to develop a holisitic metaverse framework in line with global developments.

3. The endeavour of policy makers should be to support industry-led, consensus-based multi-stakeholder approaches to the development of technology standards. Please see our response to Question 17 for further details.

Q.21. Whether there is a need to establish a regulatory framework for content moderation in the metaverse, given the diversity of cultural norms and values, as well as the potential for harmful or illegal content such as hate speech, misinformation, cyberbullying, and child exploitation?

&

Q.22. If answer to Q.21 is yes, please elaborate on the following:

i. What are the current policies and practices for content moderation on Metaverse platforms?
ii. What are the main challenges and gaps in content moderation in the Metaverse?
iii. What are the best practices and examples of effective content moderation in the Metaverse or other similar spaces?
iv. What are the key principles and values that should guide content moderation in the Metaverse?
v. How can stakeholders collaborate and coordinate on content moderation in the Metaverse?

COAI Response

1. Various laws already exist on content moderation, which will equally apply to content in the metaverse. Consequently, there is no need for the development of a separate regulatory framework to specifically govern content moderation in the metaverse.

Q.23.Please suggest the modifications required in the existing legal framework with regard to:

i. **Establishing mechanisms for identifying and registering IPRs in the metaverse.**
ii. **Creating a harmonized and balanced approach for protecting and enforcing IPRs in the metaverse, taking into account the interests of both creators and users of virtual goods and services.**
iii. **Ensuring interoperability and compatibility of IPRs across different virtual environments. Kindly give your response with reasons along with global best practices.**

COAI Response

1. The existing legal framework in India for intellectual property rights (IPR) is adequately robust to protect and enforce IPRs in the metaverse. Close monitoring of Metaverse developments is recommended to identify additional regulation needs and align new policies at a global scale.

Q.24. Please comment on any other related issue in promotion of the development, deployment and adoption of 5G use cases, 5G enabled IoT use cases and Metaverse use cases in India. Please support your answer with suitable examples and best practices in India and abroad in this regard.

COAI Response

With regard to any other related issue in promotion of the development, deployment and adoption of 5G use cases, the following points need to be taken into consideration:

I. No SACFA Requirement for LPBTS – Small Cells

1. With the proliferation of data services, the requirement of data connectivity demand has increased tremendously. To cope with the growing requirements, TSPs are deploying state-of-the-art network using low power micro cell/small cell sites (LPBTs) for providing ubiquitous coverage to those of their subscribers who are using access frequencies assigned to them. These LPBTs operate in licensed access frequency bands and are primarily deployed in existing establishments like residences, institutions, electricity poles, flyovers, foot over bridges, street light poles, advertisement hoardings, etc. with a restricted height for network coverage requirements. LPBTs, i.e., micro cell / small cell deployments seem to cause neither aviation hazards nor interference.

2. Further, as these micro cell/small cell sites are being deployed in a significant quantum and at various location categories, the SACFA applications and clearances for such sites will be complicated and cumbersome for both service providers and the WPC. This will also hinder the faster rollout of micro cells/small cells which are required for deeper

penetration of network, reduction in call drop and improvement in Quality of Services. This needs to be looked into as soon as possible.

3. A major flexibility offered by Micro Cell/Small Cell is that they can be deployed for any temporary traffic requirements and then relocated as per traffic need. **Thus, for a particular event, required coverage and capacity augmentation can be done with these Micro Cell/Small Cell at very fast pace, and later on, when Macro Sites come up for the same area or capacity need is no longer there, the small cells can be relocated elsewhere. This flexibility is an important aspect of small cell deployment for which the current SACFA Application process needs to be reviewed.**

II. Revision of EMF Limits: Follow ICNIRP 2020 Norms

1. The requirement for compliance assessment of small cells in terms of RF-EMF exposure limits may present one of the most significant barriers for rapid and sustainable network densification. This is due to the relatively larger number of small cell sites (both outdoor and indoor) that may need to undergo the assessment. Typically, small cells have a relatively small coverage footprint and operate with aggressive interference management and energy saving mechanisms (e.g. putting idle small cells to sleep). 5G uses enhanced design over LTE and even the reference signals are not transmitted continuously but with a predefined periodicity which reduces both power consumption and average power radiated on actual basis. All these factors mean that small cells usually operate well below their peak transmit powers. Therefore, RM-EMF compliance boundaries typically evaluated based on peak transmit powers create overly conservative RF-EMF limits that constrain the density of small cell deployments. For facilitating the network densification, the EMF exposure levels recently reviewed and issued by ICNIRP in 2020 be adopted in India.

2. In ICNIRP (1998) the restrictions were applied up to 10 GHZ whereas in ICNIRP (2020) it has been revised and is now applicable across the entire 100 kHz to 300 GHz range. This will ensure that exposures from new technologies do not lead to excessive temperature rise deep in the body. ITU specifically states that: - “The results of the simulation indicate that, where RF-EMF limits are stricter than ICNIRP or IEEE guidelines, the network capacity buildout (both 4G and 5G) might be severely constrained, prevent growing data traffic demand and the launching of new services on existing mobile networks being addressed.”

3. Thus, EMF exposure in India should be considered for revision and aligning with ICNIRP 2020 norms.

III. Local policies in relation to Telecom Infrastructure that impact on network performance and services to users

1. Telecom Service Providers would gain when the customer uses their services and hence making the network available to their customers is paramount for business. To roll out

physical network, deployment of BTS (using towers and other physical infra) and OFC is essential. DoT, GoI had notified the Indian Telegraph Right of Way 2016 Rules in November 2016 (RoW rules), the same has been amended on regular basis to keep pace with the requirement of technology and better user experience. It was envisaged that all the States and Union Territories will issue rules, policies, orders aligned with the RoW rules, thereby achieving the vision of Digital India and Broadband for All. National Broadband Mission (NBM) was created by GoI for the purpose of achieving the desired targets of Broadband reach to the remotest part of India. However, the pace of alignment of Right of Way Rules across all States/UTs and Central ministries is a concern. The RoW rules should be adopted and implemented in letter and spirit, especially by the local authorities in the states and UTs, which have their own bylaws and guidelines. In the Telecom Act 2023 , key provisions regarding Right of Way (RoW) and Telecom Infrastructure has been specified based on which the RoW rules will be further amended

2. NBM had created an online portal, Gati Shakti Sanchar, for processing applications for permissions related to deployment of towers and OFCs (underground and overground). This ease of business initiative is still to give complete benefits since integration of all State level and Local authorities' portals with the Gati Shakti portal has not happened.

3. Newer technologies require OFCs as a building block for better speeds and best utilization. States and UTs need to recognize the fact that infra in itself should not be seen as a revenue generating opportunity, digital connectivity is a medium and will lead to new revenue streams, directly and indirectly. Technology will support more efficient business models and enhancing productivity, thereby resulting in an increase in the state's economic growth. Keeping this basic presumption in mind, Rationalization of RoW charges is a must – digging permissions, restoration charges etc. should be facilitative in nature rather than being prohibitive.

4. Electricity is a pre-requisite for the working of the network and the industry is dependent on power suppliers for this purpose. Since the sector is a recognized industry, telecom should be given electricity under Industrial tariff category. Further, electricity connection should be provided in time bound manner without additional financial burden of last mile expenses to be borne by the industry, as currently happening in remote/hilly areas. Ministry of Power has taken some path breaking initiatives, Green Open Access and Composite Billing for customers having multiple connections. The same is required to be implemented by all states and UTs.

5. As the network elements come nearer to the users, in-building solution and Digital Connectivity within houses, buildings, public spaces (airports, malls, railway stations etc.) is critical. Ministry of Home and Urban Affairs (MoHUA) has issued an amendment to Building Bylaws, the same needs to be adopted by the states and UTs immediately.

IV. Re-evaluation of permission for Smart Grid deployment via RF Mesh using unlicensed band (865-868 MHz)

1. The Ministry of Power, vide Form 17 (Data Requirement Sheet) of Model Standard Bidding Document and Model Contract for Appointment of Advanced Metering Infrastructure Service Provider (AMISP) has allowed the use of RF Mesh technologies in both licensed and unlicensed frequency bands as permitted by WPC for implementation of Advanced Metering Infrastructure in India.

2. Currently, DoT has permitted the use of 865-868 MHz for “Tracking, Tracing and Data Acquisition Devices” and “Radio Frequency Identification Applications” without acquiring a license. It is to be noted that allowing unlicensed frequency bands for deploying a critical application **like Advanced Metering Infrastructure (AMI) at a wider scale will seriously compromise the security of the critical infrastructure apart from leading huge revenue loss to the Government and thus, such a critical application/infrastructure should be created only by the telecom companies under their license and over the licensed spectrum.**

V. Altimeter issue:

1. 5G spectrum auction including frequencies in C-Band (3300-3670 MHz) was concluded in July 2022 and frequencies were allocated in August 2022.

2. On 29th November 2022, DoT based on DGCA recommendations, issued a letter mandating large exclusion zones for 5G/IMT base stations in 3300-3670 MHz bands for Aircrafts, prescribing no C-band zone of 2.1 KMs from both ends of the runway and 910 meters from center of the runway. This was mandated to avoid any interference with the Radio Altimeters (RA) installed in the aircrafts.

3. Globally frequency range from 4200-4400 MHz is defined for aeronautical radionavigation i.e., Radio Altimeters (RAs) needs to receive and transmit signals in frequency band of 4200-4400 MHz. It is not expected to process and cause interference from frequencies outside this band in a quality and standard equipment’s.

4. The processing of signals more than 600 MHz apart in a 200 MHz authorized band establishes that such equipments namely RAs provided in aircrafts are nonconforming.

5. Further, it is pertinent to mention that 5G equipment operates in frequency band 3700-3980 MHz in US whereas in India 5G equipment operates in 3300-3600 MHz frequency band which is different than 5G band of US. Further, in this regard, Boeing and Airbus have pointed out that mitigation measures are not the permanent solution and the Permanent solution is replacement of RAs for which aircraft carriers and DGCA must act.

6. Further, Denoting complexities related to supply chain and logistics, it has been informed that retrofitting of nonconforming RAs in aircraft operational in India can be completed in 18 months and further it was also informed that this time period will commence with a mandate of Aviation regulator of India and placing orders by the aircraft carriers for retrofitting of nonconforming RAs which is a plug and play operation. Accordingly, DGCA

has been requested several times to mandate retrofitting of compliant RAs to ensure safety of aircrafts and passengers.

7. Thus, it is important to mandate all airline carriers operating in Indian territorial boundaries to replace nonconforming Radio Altimeters, to mandate completion of replacement of nonconforming Radio Altimeters in progressive manner within 18 months starting 1 October 2023, To mandate that monitoring dashboard to observe progress of replacement of nonconforming Radio Altimeters be made available on public domain, to mandate that after completion of deadline, all buffer related restrictions across all airports / airstrips should not be enforceable.

****