BIF response to TRAI CP on Digital Transformation through 5G

Preamble:

BIF an independent think tank which is working autonomously for Digital Transformation and for enhancement of the digital ecosystem, lauds the authority for coming out with a consultation paper on Digital transformation through 5G.

Please find below BIF response to the questions raised by TRAI in the aforesaid CP. We hope our response shall be helpful to TRAI in framing its recommendations to the Government.

Q1. 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.

BIF Response:

1. Yes, there is a need for additional measures to further strengthen the cross sectoral collaboration for development and adoption of 5G use cases in India.
2.
   a. 5G is the first "G" in the cellular generational hierarchy, which has stepped out of human-human interactions into the realm of machines thereby leading to huge number of machine to machine and machine to humans and human to machine interactions.

   b. Though there are benefits of 5G for individuals also, but it is the domain of machines that have got really interesting and novel use cases, which no other cellular technology has exploited before.

   c. Private 5G is considered as one of the most important and monetizable 5G use cases. Private 5G is about connecting machines together on the shop floor eg. in an automotive factory or about having enterprise wide connectivity within the boundaries of say a Hospital or a Research Institution. The unique features of 5G that caters to such enterprise wide use cases are the features of ultra-low latency and ability to support massive Machine-to Machine Communications, besides enhanced Mobile Broadband.

d. GSA on 27th Sep, 2022 reported that 889 customers across 70 countries had deployed private mobile networks at the end of August 2022. Of the total catalogued customers deploying private mobile networks in Aug 2022, LTE is used in 672 while 5G is being deployed in 354, or 39.8 per cent, of these customers[1]. The total private networks have increased to 1279 in Nov 23. On the other hand, India maybe having just a couple of such private networks at present. By virtue of being one –sixth of the global population, India should try to achieve at least around 200 Private Networks (4G and 5G) to be on par with the rest of the world.

e. One of the prime need of Private 5G use cases is the offering of direct spectrum to the enterprises. Though, this has been approved by the Union Cabinet as one of the modes of allocation of spectrum in its Cabinet approval dated 15th June 2022 but has not been done yet. This approval is in line with the TRAI recommendations of 11th May 2022 for allocation of spectrum to enterprises for Private 5G. The Government called for a demand assessment of this spectrum assignment mode for the need for direct spectrum allocation and with over two dozen large and medium enterprises having applied for it, the same has not been assigned/allocated to the enterprises as yet.

f. Some of the private 5G use cases reported by STL partners a Telecom research and consultants are as under:
   - In April 2021, Verizon announced its first European Private 5G deployment with Nokia for Associated British Ports (ABP) at the Port of Southampton, one of the UK's busiest ports that exports £40 billion worth of manufactured goods from the UK every year.
   - Spanish transport infrastructure company Ferrovial launched one of the world's first private 5G standalone (SA) networks in October 2021, to support a number of use cases at a site constructing a tunnel under the River Thames

g. In almost all the use cases for Private 5G networks, the requirement is for real time applications where meeting worst case latency is an important requirement. Such use cases are mainly related to Robotics or robot assisted manufacturing, logistics and warehousing wherein users wants real time information to deliver better services to their customers.

3. As mentioned in the Union Budget 2023-24 and also as referred to in the CP, Government of India is setting up 100 test labs in collaboration with 14 other

[1]https://gsacom.com/press-release/889-organisations-are-deploying-lte-or-5g-private-mobile-networks-worldwide/

ministries and departments to explore 5G use cases for the respective industry verticals leveraging communication technologies such as 5G/4G-Adv and IoT. The 14 ministries taking part in the 5G use case test labs are: 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.

4. There is perhaps need to further widen the scope by including other departments and ministries like Ministry of MSME, Ministry of Steel, etc, Also other use cases viz. Content and broadcast industry which requires its customers to get the content in real time, Stock trading which requires real time trading etc, could also be conceived.

5. Further, there is need to enhance focus on startups as they are capable of bringing new use cases into the mix.

Q2. 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 details of the measures taken by other countries to remove such barriers.

BIF response:

1. Yes, we anticipate barriers in development and proliferation of the ecosystem for 5G use cases and these need to be identified and addressed.

2. Indoor and in-Building penetration of 5G:

   a) 5G deployment is primarily in mid–band and higher frequency bands (milli meter wave bands). Due to RF propagation characteristics, it is difficult for 5G signals to penetrate buildings and provide indoor coverage. Thus there is need to have complementary next-generation Wi-Fi technology which can complement and match or even exceed the speeds and latencies available on 5G in the outdoor environment.
   b) As per estimates, 70-80% of mobile data usage globally happens while indoors. Hence there is need for next generation Wi-Fi 6E and Wi-Fi 7 which work on

the 6GHz band and permit 5G like ultra- high capacities and ultra-high speeds along with low latencies. This can only be made possible with license exemption being permitted in the entire 6GHz band.

c) 6GHz spectrum needs to be license exempt for holistically developing the entire wireless ecosystem without creating bottlenecks at any level. This becomes even more important as most of the devices including machines and appliances are Wi-Fi enabled and making them 5G enabled require costly upgradation of network inside the buildings. This stifles the chances of use of 5G use cases seamlessly in outdoor and indoor environments and in areas where largest amount of data is being used.

3. By enabling more License exempt bands which are the bands where most innovation takes place, it is easy to test the application and use cases with ease and without any regulatory permissions of interference with commercial 5G applications. This will help foster innovation, promotion of Private 5G and faster adoption of 5G and 6G in future.

Q3. 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?

BIF response:

1. 5G technologies are best suited for activities carried out in the outdoor environment eg. related to Transportation, Agriculture, and Education in Rural areas. This is because 5G largely works on Higher frequency band which due to poor RF propagation properties, are not able to penetrate walls and give optimum indoor coverage.
2. Agriculture had GVA of 18.3% in 22-23. Thus there is need to involve Agriculture universities and startups in creating agri-based use cases along with other engineering institutions and IT companies in a mission mode.
3. Awareness campaigns and skilling programs should be run for students, employees, and workers in new technologies viz. IT, AI, Cloud, Blockchain and ML irrespective of their core domain.
4. It is known fact that at present 5G coverage has not reached rural areas in India and it may take some time as the Operators may not be seeing the ROI in the same. A

lot of the current rural/agri requirements can be met through 4G also. There is a need to develop use cases and Apps based on 4G to start with. Once the benefits of digitalisation through such use cases is realised by the users and developers, then the use cases can be upgraded or newer use cases would become apparent which require the use of 5G. Jumping straight to 5G use cases may not yield the desired results – a gradual digital transformation through 4G initially to 5G may help.

Q4. 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?

BIF Response:

1. IoT has been in use since long. However, most of it have been in use before the advent of 5G. Different underlying connectivity technologies have been used for connecting sensors, many of which are not in the cellular domain. A number of non-cellular technologies which work on unlicensed spectrum bands have been used in this regard. Some of them are LoRA, Zigbee, Sigfox, etc.

2. Some of the IoT applications that have been in vogue are for operations of tube wells in the rural areas in 2013[2], e-ticketing using connected PoS in the state transport buses is already in vogue for last 10 years, e-challans for traffic violations by traffic police have been used since over last 7-8 years and many more.

3. Some of the measures that could be used 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 IoT smart applications and services to create new economic activities and increase employment opportunities and thereby promote economic growth are:

   a) There is need for development of smart solutions and use cases, which are able to solve real life issues of the people. Being a vast country with different areas having different issues, understanding of issues and creating unique solutions is an important aspect, for which we feel that people who understand the issues are best suited. In rural areas, several agri-startups are using a number of technologies viz. AI & IoT along with Big Data, to come up with new solutions to increase agricultural efficiencies and improve farm yields.

[2] https://www.dnaindia.com/india/report-remote-control-tubewell-with-cell-phone-1013778

b) Cyber-attacks to unsecured IoT networks are the biggest threat. According to a report from Cisco, the number of connected devices to the internet will be three times greater than the worldwide population by 2023. Our own Bharat 6G Vision document launched by Hon'ble PM earlier this year, aims to connect 25 Bn smart devices by 2030. Furthermore, with the rapid evolution of technology, hackers and their enemies can attack more things related to the internet. In fact, according to some reports nearly 98% of IoT traffic is unencrypted, leaving users' private information vulnerable. A M2M and IoT product innovator-Venafi claim that the IoT device industry had implemented encryption only in 24% of IoT devices in 2021, leaving 76% of devices entirely unencrypted[3]. CCTVs and digital video recorders were the most commonly targeted devices.

c) Undeniably, people's lack of knowledge of interconnected technology defeats their ability to secure it, and hence there is a need to educate everyone to change this situation. As the industry innovates and builds devices that integrate with the internet, it needs to learn from its mistakes. The latest updates, fixes, and patches, as well as hardening the systems, are some of the best security practices that can be utilized.

d) The users' knowledge of IoT privacy and security can positively influence users' IoT trust which can help positively influence increased use of IoT.

Q5. 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?

BIF Response:

Some of the initiatives required to be taken by the Government to spread awareness among citizens about IoT enabled smart applications are:

1. Citizens' involvement is key to the success of the adoption of Digital transformation. Government's key task is to get citizens involved in conceiving the IoT based smart solutions right at the stage of inception. This could be done if the solutions are designed in consultation with them and that would increase the chances of adoption.

2. Therefore, greater involvement of people at District and Taluka level is a must and

[3] https://venafi.com/blog/cyber-attacks-iot-devices-are-growing-alarming-rates-encryption-digest-64/

District Industrial centres may be made District Industrial Innovation centres which involves not only manufacturing industries but also teachers, students, farmers, and institutions for bringing them together for demonstration of existing IoT solutions by startups and for generation of new ideas to solve new problems being faced by citizens.

3. Incentivizing startups by way of seed funding, long term tax holidays, institutionalisation of mechanisms to support the startups from ideation to adoption of their solutions should be done at all levels right from the Gram Panchayat or village level itself.

Q6. **Industry 4.0 encompasses Artificial intelligence, Robotics, Big data, and the Internet of things are 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.

BIF Response:

1. Some of the measures that could be conceived for upskilling top management and owners of the industries are:

   (i) Basis a OECD interview conducted in 2019**,** it was found that in most of the organizations, reskilling initiatives were visibly championed by senior leaders, often CEOs and chief operating officers[4]. It was found that almost all reskilling initiatives were led by the top management. The study showed that close cooperation between the leadership and management teams in a shared responsibility manner, was the key for successful implementation of these programs. [5]

   (ii) Therefore, for driving reskilling of the workforce, BIF agree with the Authority's view on the need of skilling of top management. Even though companies now have no choice but to adopt AI for maintaining competitiveness, but still proactive efforts may lead to lesser pains for industries going forward. Ministry of Corporate Affairs in conjunction with Ministry of HRD & Ministry of Skilling & National Development may be entrusted with the task of making sure that Directors of Companies involved

[4] https://hbr.org/2023/09/reskilling-in-the-age-of-ai
[5] https://hbr.org/2023/09/reskilling-in-the-age-of-ai

in manufacturing and service sectors, have some form of exposure or a formal course for basic understanding of AI, ML, IoT, Industry 4.0, etc

2. (i) Most of the companies across the world have started upskilling of their work force but there is need to make it mandatory for all the government and PSU employees to get trained in industry 4.0 through using training facilities in Telecom sector and IT.
   (ii) NCVET has come out with comprehensive reports on "National Programme on Artificial Intelligence (NPAI) Skilling Framework". The frame work is for meeting the skilled AI manpower needs of not only industry but also armed forces and governance. There is need to adopt this framework.

Q7. 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.

BIF Response:

1. To prevent cybercrimes, there is need to first crack down on those who are involved in the cybercrimes by equipping the police and law enforcement agencies in tackling these crimes so that trust is easily built and the common man is not afraid of adopting the new technologies.

2. Other factors impacting the adoption by MSME would be the lack of knowledge, information about the various Digital initiatives and lack of resources / funding. It will generally follow once MSME see the relatively bigger companies adopting a similar approach. However, for faster adoption by them, besides the need to adopt trickle down approach the awareness and training programs could be taken up in mission mode by involving industry associations.

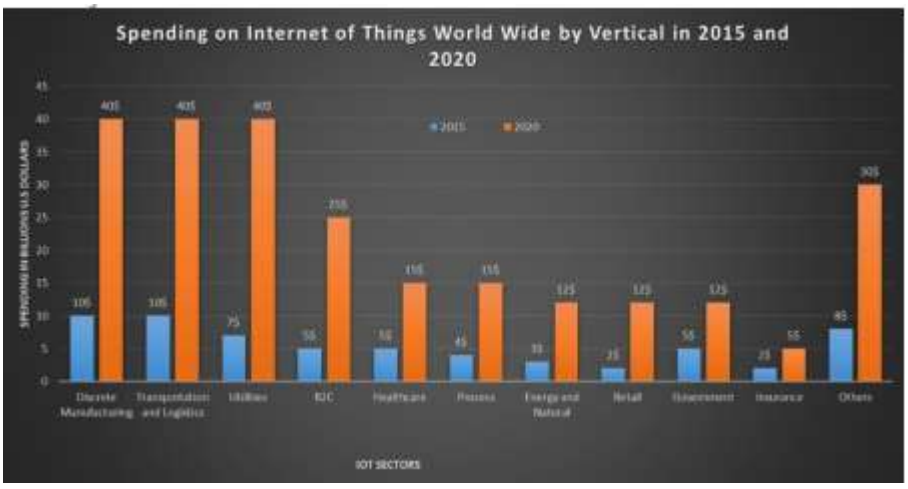
Q8. **What additional measures are required to strengthen the National Trust Centre (NTC) framework for complete security testing and certification of IoT devices (hardware as well as software) under DoT / TEC. What modifications in roles and responsibilities are required to make NTC more effective? Kindly provide your comments with justification in line with the global best practices.**

Q9. IoT security challenges and requirements vary significantly across different industry verticals. Is there a need to develop sector-specific IoT security and privacy guidelines?

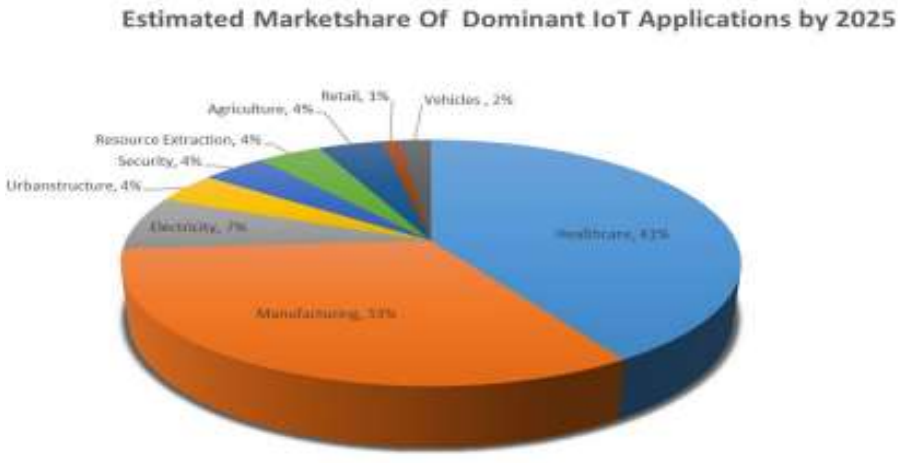
Q10. **If answer to Q.9 is yes, is there a need for a common framework and methodology for developing such sector-specific guidelines?**

BIF response to Q 8 to 10

1. In our opinion measures proposed by NTC are comprehensive and need to be adopted. No additional measures are envisaged as such.
2. As mentioned in response to Q4 it is reiterated that 76% of the IOT devices are not encrypted. In case of IoT, it is most critical to ensure that the IoT devices send data from device to server in encrypted form. According to World economic forum, there were more than 8.58 billion mobile subscriptions in use worldwide in 2022, compared to a global population of 7.95 billion and as per Exploding Topics there are 15 Billion IOT devices in 2023[6] indicating that number of IoT devices are more than mobile. And globally market share of IoT in health care is 41% while that of Manufacturing is 33%[7].



[6] https://explodingtopics.com/blog/number-of-iot-devices
[7] https://eudl.eu/pdf/10.4108/eai.16-5-2020.2304170



3. From the standpoint of challenges, health care sector is most challenging as its security has human health implications but that does not undermine the importance of other sectors. Therefore, security of IoT data is important and all the devices manufactured and installed in India must comply to NTC norms related to end to end encryption of data from device to server. It is recommended to make NTC an independent legal entity with an independent status. NTC certification of each and every device must be made mandatory for all new devices to start with.

4. However, in case of non-critical IOT applications like smart meter reading requirement, end to end encryption may be made optional, as it is likely to increase cost of IoT devices. Adoption of NTC guidelines in our opinion shall mitigate security challenges irrespective of sector and there is no need to have sector specific guidelines.

Q11. 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.

BIF Response

1. As mentioned in the response to question 8 to 10 that 76% of the devices are not encrypted. Thus encryption of End to end data from IoT device is of paramount importance from technical standpoint for critical applications. In addition, storage and processing of data must also be in encrypted form.
2. From policy and regulatory point of view HIPAA compliance for health data in US while GDPR in Europe is already being complied with. In India DPDP act has provisions for data safety for individual's Data.

3. The DPDP Act empowers the Union government to exempt any government agency from the Act on grounds like sovereignty and integrity of India, security of the state, friendly relations with foreign states, law and order management, etc. Such exemptions are doubtless essential; however, certain aspects of these exemptions are not in consonance with principles of necessity and proportionality as laid down by the Supreme Court's judgment in the Puttaswamy matter that recognised the right to informational privacy as a fundamental right and specified certain requirements to be fulfilled for this right to be restricted.

4. The government collects vital data from all citizens and is one of the biggest data fiduciaries. Hence, such exemptions must be narrowly constructed to foster greater trust among the citizens regarding sharing and processing their personal data. Moreover, clause 17 (1) (d) of the Act that denies the protections of the Act to foreign data principals must be revisited, considering its inconsistency with the protection norms provided in other progressive jurisdictions and the obstructions that might arise due to it in seamless fulfilment of adequacy conditions during bilateral and multilateral trade deals**.**

Q12. **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.**

Q13. **What measures should be taken to encourage centres of excellence to handhold startups working in the development of use cases and**

BIF Response to Q12 & 13:

12 a) Additional Policy & Regulatory Measures required to encourage R & D of IoT are:

In India the research is dependent upon IITs and other higher institutes of learning including research institutions. Participation of private sector institutions in R & D is quite low. Also the investments made by the Private Sector in R & D are miniscule as compared to that made in other leading and developed economies of the world. So, more involvement of Private Sector in R & D, more academia-industry interaction and more alignment of applied research and development being done by academia in line with the goals and needs of the industry is required.

(b) Yes. There is a need to incentivise and strengthen the startup ecosystem by promoting university level incubation. NIRF ranking lacks parameters related to incubation. One of the parameters in the NIRF ranking must be number of successful startups with more than 3 years of revenue growth or net profits etc. This

will encourage greater university and industry participation and focus on outcome based incubation and research.

13.(i) Also, CoEs need to be strengthened with additional testing equipment and should permit startups to test free of charge. There must be unified portal of test equipment availability with facility to book the test for all the startups.

(ii) Government may also think of giving grants to all the incubation centres working in this field for procurement of such equipment, maintenance, and also hiring of human resources for testing and training. We agree with para 3.78 of CP.

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 malfunctions involving IoT, drones, or robotic systems. If yes, give detailed suggestions.**

BIF response:

1. No. There is no need to make changes in relevant laws as the existing laws have provisions to deal with the issues including liability regime and effective mechanism for redressal and compensation in case of accidents, damages, or malfunctions involving IoT, drones, or robotic systems.

2. AI programs are written and orchestrated by humans. Liability can be defined as a bond that connects the wrongdoer and the various remedies under the law. Liability is what results from a mischievous act from a legal standpoint. Law lays down rights and duties and ensures fulfillment of the same. Actions or omissions are wrongful when they cause harm.

3. Liabilities of manufacturers are covered in existing laws as detailed below:

Consumer Protection Act, 1986 - An AI enabled product is meant to be safe for consumers. In case the programme does not give desired consequences for which it is designed or there is an accident out of the use of it, a consumer case is likely to be instituted claiming defective good. The petitioner needs to prove product defect was the cause of the injury so that damage can be awarded. Suit would lie against the manufacturer/programmer/ trader. The Act enables a consumer of any product or service to file a complaint in case of any unfair trade practice, restrictive trade practice, defect in goods, deficiency in service, sale of goods that are hazardous to life and safety or are in contravention of the standards laid down by the law with regard to the safety of such goods.

Indian Contract Act, 1872 -A contract made for the sale or purchase goods enabled with AI or an AI enabled programme would be governed by the terms of contract and the warranty clause mentioned therein. Where an AI enabled programme is sold to a Bank, issues arising out of the compatibility of the programme with the software in use/ conformation to functional specifications/ software provider continues to maintain an information security process along with safeguards/ for a certain period of time/ that the programme will run and perform exactly as ordained. Warranty breaches under contractual obligation gives rise to the right to claim damages but not the right to repudiate or the right to reject the contract under the Indian Contract Act. Although, condition breaches not only give rise to the right to repudiate or right to reject the contract but also the right to claim damages.

Fatal Accidents Act, 1855 - Section 1A provides for providing compensation to family members in cases where death is caused due to an actionable wrong. Under common law the vicarious liability is attached to the employer and he is held liable for the negligent act or omission of the employees in the course of employment.

Factories Act, 1948 – A Japanese employee, who was perceived as a threat by an AI robot working in a factory, which proceeded to crush him to death. Incidents like these may be common occurrence in the near future. The Act lays down the general duties of manufacturers as regards to safety in usage of substances and other articles in factories

Thus existing law have provisions to deal with issues arising out of malfunctioning, accident, damages arising out of the incidences due to AI or robotic devices.

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.**

a) Yes. It is commonly considered that due to the small-scale nature of distributed deployments, and the reduced concentration of valuable information, MEC servers are less prone to a security attack. However, as a result of the MEC boom and its critical role in the 5G evolution, this technology model will soon become a prime target for malicious actors who want to leverage this platform to disrupt its growth and in turn, use it to launch attacks against a broader user base of mobile networks.
b) Impacts of breaches in this new generation of the connected world can be vast and impactful. The MEC environment inherits risks from cloud computing and virtualized network security, by introducing the security threat vectors related to physical devices, network functions, the MEC platform and its applications. In the MEC framework, security management is required to achieve interoperability among the layers (Communication Technology (CT) capabilities, IT applications, MEC platform, devices, and edge cloud). MEC encounters security risks associated

with its deployment. MEC can be implemented at the network level using the same principles as a Mobile Packet Core[8].

c) In an attempt to mitigate the security risks, a centralized security architecture is recommended to address a hierarchical MEC security framework that covers the physical facility layer, virtual facility layer, applications lifecycle, MEC platform, user plane function and management system security[9].

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?**

BIF response:

Following are some of the policy measures which are required to create awareness and promote use of the Metaverse

1. There is need of leveraging the resources of industry participants and civil society in its efforts to generate awareness, build capacity, and ensure democratic access to the metaverse for generating awareness.

2. A diverse and relevant set of use cases is a sure shot way to promote access and awareness like UPI has been adopted by large number people in India.. Metaverse can be used in education, learning, healthcare, and telemedicine in Rural areas in India. To make it popular, Metaverse and its benefits it is necessary to take this technology to rural areas in the field of education and telemedicine.

3. The metaverse is developing; it has great promise in healthcare by fusing technologies like Artificial Intelligence (AI), VR, AR, Internet of Medical Devices (IoMD), Web 3.0, intelligent cloud, edge, and quantum computing with robots to give healthcare new directions. According to the current Medical Internet of Things (MIoT) theory, doctors in large hospitals (called "Cloud Experts") and doctors in smaller hospitals (called "Terminal Doctors") can work together to make graded diagnosis and treatment more accurate and effective. It would be easier and faster for metaverse technology to penetrate in rural India through healthcare and education.

[8] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9330515
[9] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9330515

4. Metaverse products and virtual worlds must also account for the diverse linguistic, cultural, and socio-economic backgrounds of the citizens of India. 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.

5. 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.

6. 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.

7. Further, there is need to include a strong future-led, innovation-focused subjects in the curricula of institutions through AICTE or UGC or NBA to prepare the individuals for the complexities as well as the advantages metaverse brings with itself. 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

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:**
    a. **How can users control their personal information and identity in the metaverse?**

b. How can users protect themselves from cyberattacks, harassment and manipulation in the metaverse?

c. How can users trust the content and services they access in the metaverse?

d. How can data privacy and security be ensured in the metaverse, especially when users may have multiple digital identities and avatars across different platforms and jurisdictions?

BIF Response:

1. The metaverse has a heavy reliance on the internet and other emerging technologies that will likely increase the amount and range of personal data available to exploit. The more data someone places online, the bigger their digital footprint, which means higher risk of cyberthreats and security breaches.
2. Along with traditional personal data like addresses and names, the metaverse will also collect new information like biometrics and voice recordings. This type of identifying information is a gold mine for third-party data companies and marketers—and criminals who can collect, abuse and monetize the data[10].
3. 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[11]. To ensure that regulatory frameworks are future proof and enable innovation, they should be technology agnostic.
4. Some measures that users must adopt to protect their personal information, prevent cyber-attacks, harassment, manipulations have been listed as follows:

    a) **Protect Personal Information:** Be cautious about sharing personal information with other users within the metaverse. Limit the amount of personal data in the profile.
    b) **Choose Reputable Platforms:** Only use well-established and reputable platforms that prioritize user safety. This can be done by doing research on apps and platforms before creating accounts or engaging in activities. One can also run any links through a website that checks they are safe to avoid interacting with a malicious platform. Look for reviews, user feedback, and information about the platform's security measures.
    c) **Be Cautious of Virtual Relationships:** As in the real world, exercise caution when forming virtual relationships. While the metaverse can be a place to meet new people, some individuals may have malicious intentions.

[10] https://sproutsocial.com/insights/metaverse-dangers/
[11] European Commission, An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition (September, 2023), accessible at < https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718 >

d) **Leverage Safety and Reporting Tools** Most platforms provide tools to report and block users that engage in malicious behaviour. Report any instances of cyberbullying, harassment, or any other form of inappropriate conduct to the platform's administrators and block the offender.
e) **Educate Yourself**: Stay informed about the latest security trends and potential threats specific to the metaverse. In this way, you will be better equipped to recognize and respond to risks.
f) **Keep Software Updated**: Keep on top of updates for the software and applications you use to access the metaverse. These updates often include patches that address security vulnerabilities. Outdated software can leave you exposed to various cyberthreats.
g) **Use Virtual Private Networks (VPNs)**: Consider using a VPN to access metaverse applications. A VPN encrypts your internet connection, adding a layer of security that can make it harder for hackers to intercept your data

5. As detailed out in response to Q14 also that there is no need to further regulations as existing acts namely consumer protection act and DPDP act adequately safe guard people against wilful defaults.

6. Further, Wireless Telegraphy (Possession) Rules, 1965 and certificatory frameworks such as the Mandatory Testing and Certification of Telecom Equipment (MTCTE) regime, Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021, impose additional obligations with respect to certification and testing requirements. Due to the complex structure, it is likely that certain types of devices would have to adhere to multiple standards, testing and certification requirements. Government agencies could explore harmonization of the testing and certification process which will ease the requirement of multiple certifications for devices needed to enable metaverse in India.

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.**

BIF Response

1. Yes. There is a need to establish experimental campuses where all stakeholders in the ecosystem viz. startups, inventors and researchers can develop or demonstrate

technological capabilities, innovative use cases and operational models for Metaverse.

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[12] 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[13]. Dubai International Financial Centre[14] (**DIFC**) launched a Metaverse Accelerator Programme to support innovative metaverse start-ups by helping them explore partnerships. Singapore government (through its Personal Data Protection Commission)[15] 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.
3. Today, involving users in research, design and innovation processes constitutes a fast growing topic globally and the concept of living labs has come up. Living labs are open innovation ecosystems in real-life environments using iterative feedback processes throughout a lifecycle approach of an innovation to create sustainable impact. They focus on co-creation, rapid prototyping & testing and scaling-up innovations & businesses, providing (different types of) joint-value to the involved stakeholders.

4. MIT Sloan living labs are of three types:

   a) Campus to Campus

[12] https://www.thehindu.com/news/national/karnataka/centre-of-excellence-in-metaverse-becomes-a-reality-in-mysuru/article66226244.ece

[13] https://www.arabnews.com/node/2251326/corporate-news

[14] https://innovationhub.difc.ae/programmes/Metaverse-Accelerator-Programme

[15] https://openloop.org/programs/ai-transparency-explainability-singapore-2/

This type represents research originated on the MIT Campus, that is then applied to the MIT Campus.

b) Campus to Market

This type of living lab represents research that is tested and refined by utilizing the MIT campus, and then applied directly to the market.

c) Market to Campus

This type of living lab originates from an external entity, and then it is tested on the MIT Campus, and then applied to the MIT Campus.

5. EU has 'Future Internet Research and Experimentation' and IoT test beds. Work is going on to properly articulate Living Labs with FIRE and IoT testbeds in order to make sure that innovative services enabled by the Future Internet will meet the expectations and desires of user communities.
6. Globally such experimental labs are already in existence and such type of labs or center for excellence, and test beds are useful in involving communities and creation of products by involving users into the design and innovation.
7. India may also replicate the concept of living labs, FIRE, and IOT in CoEs to make it possible to have well researched, standard products to the market.

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.**

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.**

(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.

BIF response to Q 19 & 20:

Metaverse Standardization

1. The metaverse focus group recently formed by the International Telecommunication Union (ITU) with aim to lay the groundwork for technical standards to help everyone benefit from metaverse services as need for interoperability, integration of real and virtual world. 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. 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. XR technologies which is core to metaverse is nascent. A global effort involving industry-wide cooperation will be important to build interoperable metaverse. Industry alliances such as the Metaverse Standards Forum and the Open Metaverse Interoperability Group are working to address broader needs for interoperability standards. The close interdependencies between metaverse and IoT sectors also motivated oneM2M to explore these issues[16]. Several organizations from Korea, a country that is firmly on the metaverse path, are involved alongside oneM2M members from other countries. The Linux Foundation is focused on fostering innovation through open source, has established the formation of the Open Metaverse Foundation (OMF)[17] with a mission to provide a collaboration space for diverse industries to work on developing open source software and standards for an inclusive, global, vendor-neutral and scalable Metaverse.

3. In India government has supported a forum for telecom standards. One forum for a diverse nation may not fit well. Therefore, government must support various forums which have credible track record, independent, and work in diverse areas of telecom and IT sector.

4. Further, if the technology or products based on it are not aligned with the interests of people the it will be difficult to push through in the market. Globally a need is being felt to involve people in the ideation and innovation so that the products are able to resolve real life problems. Therefore, for bring competition there is need to have standards for faster innovation and competitive environment. And for making this to happen there is need to focus on standards in metaverse. For standards, both Indian companies and premier institutions in India like IITs and NITs may be assigned the role of participation in ITU and other industry alliances for global standards. For meaningful contribution in standards there is need to have

[16] https://www.thefastmode.com/expert-opinion/30064-standardization-is-key-for-metaverse-success
[17] https://c212.net/c/link/?t=0&l=en&o=3760027-1&h=209313045&u=https%3A%2F%2Fwww.openmv.org%2F&a=Open%C2%A0Metaverse+Foundation

institutionalized system for facilitating filing, granting, and maintaining global patents as patents enhance credibility to proposals at these forums.

5. The existing legal framework in India for intellectual property rights (IPR) is adequately robust to protect and enforce IPRs in the metaverse. The Indian Copyright Act, 1957 penalises the act of knowingly infringing or abetting infringement of copyright or any other right granted under the Copyright Act. Similarly, under the Trademarks Act, 1999, the registered proprietor of the trademark is entitled to certain exclusive rights in relation to the use of the trademark for the goods and services it was registered for. Further, the Patents Act, 1970 grants an exclusive right to a patentee to prevent third parties from using the patented product or process without any authorisation.

6. Though, government of India has made it easy and cheap to file patents in India but it is very costly for any start up to fund filing, granting, and maintenance of patents. For one global patent it costs about $31000 for 20 years patents in USA and Europe. Thus for any startup it is difficult to go for 100 patents as it may cost Rs 30Crores. Therefore, it is proposed to create a body within the ambit of MEITY or DOT to fund patents and device mechanism of sharing revenue from patents with patenting organization.

7. For prototype creation a special fund may be created to finance start-ups. There is suitable mechanism available in India for identification through **Digital Communication Innovation Square(DCIS) or other such bodies** and selection of 20-25 startups which having good track record.

8. Governance Framework

    1. The metaverse does not exist in a regulatory isolation and therefore, there is no need for a specific regulatory framework to govern the development and use the metaverse as. The current legislative framework effectively governs 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.
    2. The government may consider incentives in the form of tax subsidies to drive holistic development and adoption of the metaverse products and also to encourage collaborative development of metaverse technologies. Further XR

and related products could be considered in the Production Linked Incentive (PLI) scheme to attract XR related hardware manufacturers.

3. For example, Dubai Municipality has announced a partnership with private companies and investors to create a futuristic, human-centred city in the metaverse called 'One Human Reality'. South Korean government has announced a $186.7 million package to simulate a government led metaverse ecosystem, with a focus on encouraging young talent and fostering a culture of convergence.
4. There is greater need today for government, industry participants, civil society, technology experts, users and other relevant stakeholders to come together in various ways to determine how the metaverse is governed, with the aim of promoting dialogue and discussion, enabling sharing of information and best practices, and developing joint standards or guidelines for effective governance.

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?

1. No. There is no need to establish a regulatory framework for content moderation in the metaverse. Existing laws are more than sufficient to deal with it.
2. Following are the existing laws which have provisions for protecting against the harmful or illegal contents:
   (i) Section 67B of the Information Technology Act, 2000 provides punishment for publication and transmission of child pornographic material or any other obscene content, and content depicting children as engaged in a sexual act in any electronic form.
   (ii) Section 12 of the POCSO Act provides punishment for sexual harassment. Any person committing an offence of sexual harassment shall be punished with imprisonment for a term which may extend to three years and with a fine.
   (iii) Section 13 of the POCSO Act explains the use of children for pornographic purposes that are prohibited under law. Section 13 provides that any person who uses the child for sexual gratification in any electronic media either for his personal use or for distribution can be said to have used that child for a pornographic purpose. It includes obscene representation of the child, display of sexual organs of the child, and display of a child engaged in a sexual act.
   (iv) Section 14 of the POCSO Act provides punishment for using the child for pornographic purposes. A person committing an offence under section 13 of the Act shall be punished with imprisonment for a term not

less than five years and with a fine. On second or subsequent conviction for a term not less than seven years and with a fine. If the person also commits an offence under section 3 or section 5 or section 7 or section 9 by himself participating in the act of pornography shall be punished under section 4 or section 6 or section 8 or section 10 respectively in addition to the punishment under section 14.

(v) Section 15 of the POCSO Act provides punishment for storing pornographic material which involves a child. If a person stores or possesses the material with the intention to transmit or distribute the same without reporting it to the authority will be liable to pay a fine of not less than Rs.5000. On second or subsequent conviction with a fine of not less than Rs.10000. If a person stores or possesses the material for transmitting or displaying or distributing the same except in a manner prescribed under law for reporting the same will be punished with imprisonment for a term which may extend to three years or fine or both. If a person stores or possesses the material for a commercial purpose shall be punished with imprisonment for a term not less than three years but may extend to five years or a fine or both. On second or subsequent conviction for a term not less than five years but may extend to seven years or fine or both.

(vi) Section 16 of the POCSO Act provides that abetment to commit any of the above offences shall be punishable.

(vii) Section 153 A of IPC deals with hate speech. If any person commits an act which leads to promoting enmity between different groups on different grounds and which are prejudicial to the maintenance of harmony.

(viii) Section 419 of IPC deals with cheating by impersonation. Under the section, any person who commits cheating by impersonation will be punished with imprisonment for a term which may extend to three years or fine or both.

(ix) Section 500 deals with defamation. Any person who commits defamation will be punished with simple imprisonment for a term which may extend to two years or with a fine or both.

(x) Section 506 of IPC deals with criminal intimidation. A person who commits criminal intimidation will be punished with imprisonment for a term which may extend to two years or with a fine or both.

(xi) Section 292 of IPC prohibits the possession, sales etc. of obscene material.

3. The (Indian) Information Technology Act, 2000 read with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Rules) prescribes content related due-diligence requirements for intermediaries and requires them to inform the user to not host, display, upload, modify, publish, transmit, store, update or share a variety of information that may be harmful including information that belongs to another person, is obscene, pornographic, paedophilic, invasive of another's privacy, is insulting or offensive, is harmful to child, deceives or misleads the reader, threatens national security, contains any harmful code or virus, or is otherwise violative of any laws in force.
4. Therefore, BIF response to Q21 is that there is no need to have fresh regulatory framework for content moderation in metaverse. However, multilateral consultation started by government needs to be continued and strengthen further.

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?**

BIF response:

Since response to Q21 is No, hence Q22 needs no response.

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.

BIF Response:

Issue dealt in response to Q 19 and 20

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.**

BIF Response:

The importance of making license exempt new spectrum bands, particularly the 6GHz band is of paramount importance for depaloyment and adoption of 5G use cases in indoor environs, 5G IoT use cases and Metaverse use cases in India.

This is because the 1200MHz available in the 6GHz band is the only spectrum band that supports large carriers/channels of channel sizes of 320MHz and 160MHz, thereby permitting adoption of unique 5G & Metaverse use cases which are bandwidth intensive /hungry, details of which are given below.

Opening of the 6GHz band for unlicensed use will enable Metaverse:

1. The content driving metaverse adoption is currently and in the future periods as well be consumed over fixed networks through Wi-Fi, which makes it critical that fixed networks have adequate technical capabilities.

2. While the 2.4 GHz band is already crowded, the 5 GHz band may soon face the same issue with the increasing demand for data. Existing wireless technologies are unfit for the metaverse. The current generation of WiFi suffers from high latencies and congestion after connecting multiple devices.

3. To enable a metaverse ready network, following will be the key requirements:

- **Predictable low latency and jitter**
    - First, predictable low latency and jitter is a must for smooth AR and VR experiences. This not only improves performance (i.e. no lag or buffering), but is necessary to protect against motion sickness. For reference, today

almost 150ms of latency is acceptable in video calls. This needs to improve by an order of magnitude for a cloud based VR service.

- **Sustainable throughput**
  - Sustainable throughput can be delivered, especially in cases where there is remote rendering for the headset, either using the cloud or a local computing device (e.g desktop/laptop). VR headset places a high-resolution (4K-8K) screen very close to user eyes as a result of which every distorted pixel will matter.
  - Most video call apps use a minimum of about 500 Kbps for one-way standard definition calls and a maximum of around 1.8 Mbps for one-way high-definition video. In comparison, a good metaverse experience will need almost 25 Mbps of ***symmetric*** throughput. Upload will almost be the same as download as all users will transmit and experience at the same time.
  - Low Power Consumption and Thermals**:** The headset battery should not get heated like a phone, given close proximity to the user's face and it could cause burns. And finally, power consumption because of high network requirements should not drain out the battery (for example, the AR spectacles are envisioned for day long use).

4. While access to 5G will support the development of the metaverse by providing the speed and power and will be the critical enabler, however, 5G installed directly in the headset, cannot be expected to meet the requirements as the headset would get too hot and the battery would get consumed too fast. Wi-Fi can complement 5G in helping meet these requirements
   a. In the envisioned future, the handheld compute device will receive 5G, which will then connect to the headset using Wi-Fi
   b. Unfortunately, existing unlicensed spectrum in the 5 GHz and 2.4 GHz band is not good enough for this
      i. First, channels are small (20 and 40 MHz) so throughput is not high
      ii. Second, lots of legacy devices use these bands because of which backward compatibility needs to be maintained
5. 6 GHz can address the above requirements
   a. As discussed in the White Paper on 6 GHz Band ("White Paper") by the Telecom Regulatory Authority of India ("TRAI"), 6 GHz enables good coverage, capacity, network performance and bandwidth.
   b. As 6GHz is a greenfield spectrum so backward compatibility with legacy devices is not needed, this gives the opportunity to adopt the state of the art technologies/ standards. Further, there are large (80 and 160 MHz) channels in 6 GHz that provide lower latency, power savings and higher throughput, which are all essential to AR/VR and wearables. There have been two studies in India, which are helpful references:

      i. Study by Prof. Rekha Jain from IIM-A, has estimated that the economic value of unlicensed spectrum bands in India is significant

for 2025: INR 12,69,998 crores (for GDP at current prices). This is nearly 6% of the projected GDP in 2025. The contribution of the 6 GHz band is expected to be 9.5% to the total economic value in 2025.

ii. In Oct 2021, Broadband India Forum released a co-existence study, which concluded that RLAN operation in India for all three RLAN device classes [Low Power Indoor (LPI), Standard Power (SP) (indoor/outdoor) with Automated Frequency Coordination (AFC), Very Low Power (VLP) (indoor/outdoor)] in the entire 6 GHz band will not cause harmful interference to Fixed Satellite Services or Fixed Service incumbents.

iii. As mentioned above and also highlighted in the TRAI white paper, the 6 GHz band is much wider than the 2.4 GHz and 5 GHz bands and supports low latency, high throughput, security services and better speeds. These features are critical for the metaverse which involve multiple users and congested networks. Wider channels also enable a better user experience and longer battery life for AR/VR head mounted displays. However, use of the 6 GHz band is currently limited, as it is a licensed band in India. Internationally, over 35 countries have chosen to delicense the 6 GHz. They include the United States, UK, Korea, Brazil, UAE, Saudi Arabia and the countries in the EU. The rationale for delicensing has been to enhance benefits to citizens while reaping the benefits of economic growth in their economies.

iv. Opening up the full 6GHz band will enable domestic developers to compete with their counterparts in other jurisdictions and will ensure that India remains competitive in the metaverse market. Service provision in unlicensed bands is also less expensive and is likely to spur further innovation by small businesses and start-ups. Policymakers should consider un-licensing these bands as it would have varied benefits including mobility, cost effectiveness, and seamless compatibility with smart devices and will unlock untapped economic value in the Indian market.

6. **Open access telecoms policies will enable India to be truly successful with the metaverse.** This will attract greater foreign investment in terrestrial fiber networks to support the efficient flow of this metaverse content. Where foreign entities are investing in subsea cable and related connectivity and data caching infrastructure solely to support their own products and services in India, a lighter touch approach should be adopted by policy makers and regulators, which is tailored to circumstances where the infrastructure is for private use only, rather than forcing these entities to either get a managed service from an Indian licensed operator or apply for a full blown telecommunications license in India.