VIL/AH/RCA/2024/002

January 22, 2024

Advisor (Admin)
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawaharlal Nehru Marg (Old Minto Road),
New Delhi – 110002

Kind Attn: Ms. Vandana Sethi

Subject: Comments on the TRAI's Consultation Paper on "Digital Transformation through 5G Ecosystem" dated September 29, 2023

Dear Madam,

This is in reference to the TRAI's Consultation Paper on "Digital Transformation through 5G Ecosystem" dated September 29, 2023.

In this regard, kindly find enclosed herewith comments from Vodafone Idea Limited on the above-said consultation paper.

We hope our comments will merit your kind consideration please.

Thanking you,
Yours sincerely,

For **Vodafone Idea Limited**

Anjali Hans

Anjali Hans
Senior Vice President - Regulatory & Corporate Affairs

Enclosed: As stated above

VIL Comments to the TRAI Consultation Paper on "Digital Transformation through 5G Ecosystem"

At the outset, we are thankful to the Authority for giving us this opportunity to provide our comments to the TRAI Consultation Paper on "Digital Transformation through 5G Ecosystem" dated September 29, 2023.

In this regard, we would like to submit our question-wise comments for Authority's kind consideration, as follows:

Question-wise Comments

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.

And

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.

VIL Comments to Q.1 and 2

1. The growth of telecommunication services, such as mobile networks and internet connectivity, has facilitated the expansion of businesses and entrepreneurship, particularly in sectors like e-commerce, IT services, and digital payments. The telecom networks are propelling digital wave in the society, leading to huge push to new line of businesses, jobs and increase in economy along with propelling start-ups and unicorns. The telecom infrastructure will continue to be the primary gateway to the internet and plays a pivotal role in use cases spread across various sectors. It is important that telecom services should be treated as essential service like water and electricity and be accorded ICT the status of essential national infrastructure.

2. Beyond such infrastructure, the use cases for 5G are also projected to generate significant economic growth. In particular, the increased speed, capacity, and functionality of 5G networks will help to enable the next generation of data-enabled innovations such as the Internet of Things (IoT) and artificial intelligence (AI).

3. **Need of Cross-sector Collaboration:**

    a. The biggest value proposition of 5G will be in ushering innovative use cases across industries. Cross-industry collaboration will be key to drive the launch and adoption of 5G services. Telecom operators, manufacturing companies and network equipment vendors and other start-ups/companies have been showcasing variety of 5G-enabled use cases.

b. 5G is set to introduce smart manufacturing and industrial automation to further expand the Industry 4.0 use cases in the country. In healthcare, 5G is expected to accelerate digitization of hospitals by supporting faster data transmission and usage of immersive technologies in training for example. In the rural areas, 5G has the potential to enhance remote consultation and diagnosis, benefitting a larger part of the population.

c. The TSPs have been collaborating/partnering technology companies and leading players in various industries to trial 5G business-to—business (B2B) uses cases. The advanced manufacturing and automotive verticals are leading in 5G collaborations, followed by Technology and Media. Among use cases, autonomous/connected vehicles, smart manufacturing/industrial automation and immersive content are key ones.

d. **5G Use-cases by VIL:** VIL carried out various use-cases and collaborated with other sectors in the preliminary stages of testing and thereafter. Some of such collaborations are listed below:

   i. Under the guidance of TRAI, conducted a 5G trial in collaboration with other sectors at locations like Kandla Port in Gujarat, MG Road Metro Station in Bengaluru and smart-city Bhopal.

   ii. Partnered with Ericsson to showcase 5G's potential to enable access to healthcare in remote parts of the country.

   iii. Partnered with L&T Smart World & Communication to test private 5G network use cases leveraging L&T's Smart City platform.

   iv. Partnered with Athonet, an LTE and 5G solutions platform provider, to test 5G-based solutions for Industry 4.0.

   v. Partnered with US-based Ciena on 5G solutions to prepare for commercial 5G rollout.

e. Further, 5G is expected to boost government service delivery and enhance the quality of life for citizens. Improved safety and security measures through HD security cameras and VR glasses for rescue operations, smart utility services, and high-speed connectivity in public places will help to significantly enhance the digital quotient of the nation. It will advance societies, enhance experiences, transform industries, and pave way for smart agriculture, smart manufacturing, smart healthcare, and in turn, smart cities. The extensive collaboration across industry verticals and their regulators is essential to leverage the potential of 5G in India.

4. However, despite the huge push to various use cases and connectivity testing in various areas like Port, Metro, Airport, Smart city etc., there are still no substantial 5G use cases available in the market. This indicates that lot more needs to be done in terms of cross-sector collaboration so that specific use cases are launched by sector specific entities, thereby benefitting the society as a whole.

5. **Measures required to strengthen the Cross-sector Collaboration:** India being a diverse market, has multiple barriers in development of ecosystem and adoption for 5G use cases, which need to be addressed. As 5G impacts a wide range of industries and their exponential growth, considering the above, additional push is required for collaborative approach involving all stakeholders –

companies across various sectors, various Departments of Government, TRAI TSPs, network equipment vendors and technology players, etc. Following additional measures are suggested to enable and strengthen cross sector collaboration:

a. **Cross-sector Strategy groups:** A centralized committee, encompassing representatives from government, industry, and other sectors is required to foster collaboration, define priorities, and allocate resources efficiently. The need of the hour is to bring more and more services under the digital umbrella and accessible through mobile apps.

b. **Spectrum Leasing:** Spectrum leasing can support by providing some portion of the exclusively licensed bands in a given geography to other non-access users through leasing and has an untapped potential presently.

c. **Regulatory Sandbox framework:** Many 5G use-cases may require testing in a protected environment due to some restrictions in licensing/regulatory norms, to establish their value to the consumers and society. The Regulatory Sandbox framework needs to be put in place to help and enable testing of innovative business models, products and services through TSPs, while understanding their impact from a regulatory perspective.

d. **Incentivization:** High regulatory burden leads to higher pricing for customers including enterprises, which potentially discourages the enterprises to be involved in the development of new use cases. An incentive mechanism for identifying innovative 5G use cases and expediting 5G rollout is of paramount importance, hence, the Government can look at incentivizing key stakeholders working on 5G to pave the way for wider socio-economic reforms in the country. High regulatory levies and taxes that are sector-specific have a disproportionate impact on operators and in turn, on the consumers and need to be reviewed. Incentives to invest will also ease out the enormous financial burden in rolling out newer technologies.

e. **Roll-out of connectivity:** As the 5G connectivity roll-out continues, the network would be highly dependent on backhaul spectrum and network densification which is reliant on small cells.

    i. Small cell Densification: Though the marginal cost of small cell equipment is generally lower than deploying a macro base station site, however, as large number of small cells would be required to be deployed to provide additional capacity in densely populated areas for 5G connectivity, the total expenditure would be quite substantial.

    ii. Backhaul Network: The network densification through growth in the number of small cell will increase the traffic pressure on backhaul networks. While fiber-based backhaul can offer unlimited capacity and low latency that are perquisite for 5G applications, however, the present available backhaul solutions with operators will not be enough. The issue with the availability of adequate amount of high capacity backhaul spectrum needs to be addressed to support 5G.

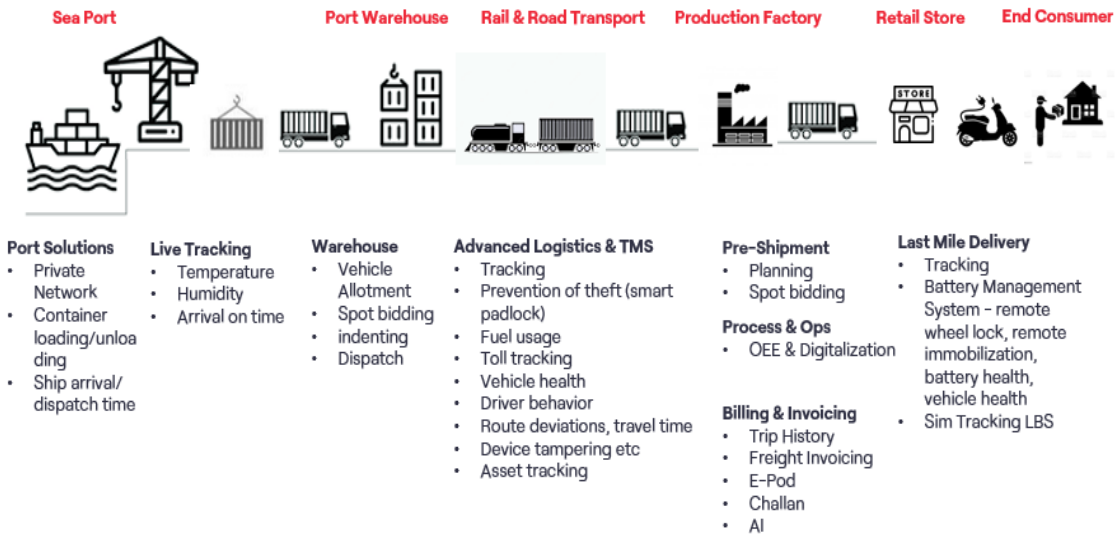
    iii. Therefore, for a developing country like India, it is expected that requirement of backhaul spectrum and small cell deployment growth would be huge and outpace global standards also.

f. **5G Roadmap:** The Government should define a roadmap which can be referred across sectors to help the stakeholders develop an idea and timelines to work on such new technologies.

g. **Alignment with sectoral regulations:** Since every sector is governed by a set of their specific regulators and government entities, it is important that all such agencies are aligned towards achieving the complete potential of 5G technology. The efforts must be made to work with inter-sectoral regulatory bodies to deal with regulatory issues emerging due to the development of 5G Use Cases in different sectors. The regulatory bodies shall intervene in conflict situations and also help formulate policies that will promote innovation in development of 5G Use Cases and local entrepreneurship in the country.

6. **Use Case and Related Challenges:**

a. The following use case of Industry 4.0 is being used as an illustration. This depicts the journey from the time the raw material consignment arrives at a port in a container to the time it is dispatched as a finished product to the end customer via last mile delivery.



b. In case of above scenario, we would like to highlight that there are multiple constraints/challenges related to cost, connectivity, collaboration, etc. which need to be addressed to fully benefit from this use case when implemented on-ground. Some such challenges and suggested solutions are listed below:

Sl. No.	Constraint	Challenges	Suggested Measures
1.	Cost/RoI	• Large CAPEX requirements with unclear ROI. • Long gestation period.	• Incentivization programmes/ subsidies to promote adoption of Industry 4.0. • Creation of Carbon credit Monetization Schemes.
2.	Capability	• Legacy Machines/ Proprietary protocols that are difficult to smartify and connect.	• Machine Modernization Policies and Funds.

		• Lack of appropriate Skill and technical knowledge.	• Upskilling/Training Programmes - Skill India/ Academic Programmes.
3.	Collaboration	• Lack of alliances and expert collaboration between ecosystem. • No regulatory framework.	• Set up Work streams/ Task forces with IT/ Telco/ OEM experts to create viable and repeatable Industry 4.0 application and solutions/ Labs/ CoEs • Regulatory framework/ Policies and guidelines for Interoperability, standardization and cybersecurity • Develop Startup ecosystem.
4.	Connectivity	• Lack of High Speed Network Infrastructure.	• Fiberization of sites. • Implementation of Edge Computing.

7. **The above suggested measures, would be relevant for and applicable to numerous use cases and are required to further strengthen the cross-sector collaboration for development and adoption of 5G use cases in India.**

8. In addition to above, this telecom industry faces certain challenges and barriers which indirectly impact the growth of telecommunication including 5G. Following are some such barriers development of ecosystem of 5G use cases:

   a. **Levies on TSPs:** The Indian telecom sector is amongst the most competitive in the world and has one of the lowest tariffs globally. The telecom sector is also subject to huge levies like Licensee fee including USO levy, GST etc., which increases the cost for the operators. These levies wipe away considerable amount of revenue earned by the TSPs. Further, the sector is also laden with dual levies, wherein charges paid by an operator for input services, is also considered a revenue for the purposes of license fees, etc.

   b. **Spectrum prices:** Telecom sector is also burdened with huge spectrum prices, which include auction price of access spectrum as well as % of AGR based pricing for backhaul spectrum. These prices are amongst the highest globally, when compared with many matured markets.

   c. **Right of Way:** There is a huge dependency on ROW to deploy the network infrastructure in the country. RoW costs vary hugely across different states/UTs and within different areas of states. This is one such factor which greatly influences the cost of network deployment and should be one of the primary indicator. The Telecom Act 2023 carries several forward looking provisions to ease the ROW challenges, including formulation of rules to prescribe/lay down the ROW charges.

   d. **Public Funding:**

      i. The Universal Service Obligation Fund (USOF) is met by resources raised through a 'Universal Access Levy (UAL)', which is a percentage of the revenue earned by all the operators under various licenses. However, presently the term “Universal” is being addressed through a narrow and short-term goal of extending coverage to subscribers of

a single TSP. Public interest outcomes would be better achieved if the projects funded by Public money (e.g. USOF) are made mandatorily accessible to subscribers of all TSP who are the contributors to the fund.

ii. This present arrangement whereby the project serves the purposes of only subscribers of one TSP, cannot be called "universal" as it creates assets only for use by a single TSP rather than providing connectivity to the public hence, it is not in interest of general public.

iii. The funding provided to only one TSP doesn't leads to universal service, instead, it gives undue advantage to a TSP with a good financial health and allows them to build network and assets on their balance sheets giving coverage to their own subscribers instead of general public, basis public money or special dispensation from Government.

iv. **Therefore, it is most important to prescribe a definition of 'Universal Connectivity'. We recommend that Universal Connectivity should be defined as Digital connectivity from all the TSPs providing wireless access service, serving public at large.** These comments in detail have also been provided to TRAI's consultation paper on "Telecommunication Infrastructure Sharing, Spectrum Sharing, and Spectrum Leasing" issued on 13.01.2023.

e. **Pricing of Smartphone:** The primary mean to access the internet and 5G use cases is heavily dependent on digital devices (smartphones). However, penetration of 5G phones as well as cost of smartphones for low-income groups, is a very big challenge. A smartphone connected to internet is essential for civic & cultural participation in today's digital world and to be updated with advanced technologies.

f. **Conversion of 2G consumers to 4G/5G:** A substantial part of the citizens in the country are generally using older technology i.e. 2G and are not able to access the new generation technology i.e. 4G and 5G despite availability of connectivity. The inability of users to switch to smartphones on account of the cost of these devices, also leads to the users continuing on older technology and hence, not using digital services and most likely ending up being not updated on latest digital technologies and services. Such barriers further increases digital divide as well as would also impact ecosystem for 5G use cases and thus need a concerted effort and push from the Government to get resolved.

g. **Review of KYC norms to cater to /facilitate various 4G/5G telecom solutions:**

i. Many solutions are being offered to businesses that comprise not just telecom connectivity, but digital platforms such as hosted cloud telephony platforms, integrated solutions combining services of 2 -3 licenses, and enablers for machine –to-human citizen-centric applications.

ii. Such solutions do not use the bulk mobile connections/SIMs in the conventional sense and to that extent, the proliferation of these solutions in the market is being inhibited by trying to fit the same into the conventional regulatory/KYC requirements that have been laid down by DoT especially the instruction to mobile operators to carry out the KYC of end-users.

iii. **As many solutions cannot be blanket-fitted into bulk mobile connection category or M2M category as formulated by the DoT we request TRAI to take up the matter with**

DoT to not to insist on end-user list requirement for such solutions to facilitate the digital transformation of businesses and their offerings to consumers in the country through these solutions.

h. **Privacy and Data Protection:** This is a major concern to consumers and also poses public security vulnerabilities. Social Media has also created new vulnerabilities. Government should come out with effective but easy to implement mechanisms to protect user data and privacy.

i. **Physical Security of 4G/5G Infrastructure:** The Government needs to introduce policies to address incidence of vandalism and theft as it may get worse with high density 4G/5G networks. The Telecom Act provides that Government can declare any telecommunication network, or part thereof, as Critical Telecommunication Infrastructure, damage to which would be punishable with imprisonment for a term which may extend to three years, or with fine which may extend up to two crore rupees, or both. We recommend that 4G/5G infrastructure may be declared as critical infrastructure. We recommend promulgation of guidelines on vandalism proof design, installations and real time protection of infrastructure components.

9. **All the above mentioned factors play a very important role in TSPs ability to provide quality and affordable connectivity and to support development of ecosystem for advanced technologies. We strongly feel that rationalization of these aspects would certainly go a long way, in helping the operators' 5G rollout and the consumers to benefit from newer technologies.**

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?

VIL Comments to Q.3

1. As policymakers seek to promote 5G deployment, there are certain key areas where sound policy approaches and government action is essential. These include innovation, investments, access to resources, etc.

2. **Policy Interventions/Schemes:**

   a. **Handset Subsidy:**

      i. There is a need to have a central and pan-India based scheme which can cater to the users who are in bottom of the pyramid and using feature phones. These consumers having these feature phones are generally using older technology i.e. 2G and are not able to access the new generation technologies i.e. 4G/5G, despite availability of connectivity.

      ii. There is issue in upgrading of phones from feature phones to smartphones due to affordability and starting price point of smartphones. Also, large number of users may not have enough money to buy a smartphone.

iii. This leads to the users continuing on older technology and hence, not using digital services and most likely ending up being not updated on digital technologies and services. This is the major factor which causes digital divide.

iv. There has to be a concerted effort and push required with incentives and subsidy from Government, to address it.

v. One of the alternatives could be that the Government provide funds as handset subsidy to consumers at large, through their concerned TSP, for giving up feature phones and purchasing subsided smartphones. This can help such consumers to start digital journey thereby, bridging the digital divide. If such stimulants are not taken timely, the digital divide will keep on increasing despite advancement in technologies.

vi. Transitioning of users from feature phone to smartphone will increase the ability of the rural masses to benefit from newer technologies like 5G and participate in the market economy, directly leading to better earnings and also bridging digital divide. Further, it will also expand ecosystem of other sectors and players having digital services which rely on consumers using mobile broadband services over smartphones.

vii. This scheme can be funded through the existing corpus lying in USOF and would also meet the objective of Universal connectivity for the low income consumers.

viii. **We urge the TRAI to recommend to the Government, for coming out with a handset subsidy scheme through concerned TSP, to support marginal consumers in upgrading their handsets from feature phones to smartphones.**

b. **Government/public funding to complement private sector investment and accelerate the rollout of 5G infrastructure:** The Telecom Service Providers (TSPs) should be mandated to share infrastructure that has been funded, either partially or fully, by the Government through USOF or otherwise, with other TSPs on commercial but wholesale rates, i.e. lower than retail rates. This will ensure fairness for all parties concerned, given that USO funds are contributed by all telecom operators.

c. **Accessibility to BBNL fibre on commercial grade basis:** BBNL has already laid out vast route length of fibre across the country, which is available in the under-covered and uncovered rural/semi-urban areas as well. This fibre should be made available to the TSPs but, on a commercial grade SLA basis i.e. with >99.9% uptime along with penalty clauses. Also, the fibre has to be made available on market pricing applicable to such rural/semi-urban areas. Accordingly, relevant provisions of Policies / guidelines / Master Service agreements / Acts should be amended.

d. **Utilize existing USOF funds for tower fiberization of under-covered and uncovered areas:**

i. The Government has launched mission Antyodaya thereby aiming to bring rural or poorest of poor public to get the same services as would be with the public in urban/semi-urban areas. To achieve Antyodaya in Telecom, there is a need to encourage and incentivize service providers for effective utilization of the BharatNet infrastructure in provisioning

of connectivity to Institutions/households/ individuals. This can be achieved by fiberization of towers in rural areas in the following manner.

ii. USOF should also be provided for fiberization of towers in under-served rural areas as well (say in cases where the towers have tenancy of at least two TSPs). This will help provide meaningful next generation telecommunication services and uplift digitally deprived areas and reduce digital disparities in the near future.

3. We further submit that apart from the stakeholders and policy makers of telecom industry, the start-ups and entrepreneurs should also gear up equally in providing the innovative solutions to fully exploit the benefits of 5G.

4. **Hence, the policymakers need to take a holistic approach and consider measures that take into account principles from every area.**

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?

VIL Comments to Q.4

1. Promotion of use of IoT technology and its infrastructure in rural and remote areas, especially through 5G-enabled applications, can significantly contribute to economic growth, employment opportunities, and overall development of the country. Following are some policy measures that can be implemented to facilitate this:

   a. **Infrastructure Development:** Investment in the development of robust and widespread digital infrastructure, including fiber connectivity & 5G networks, in rural and remote areas.

   b. **Financial Incentives:** Provision of financial incentives, subsidies, or tax breaks for businesses and service providers to develop and promote IoT applications specifically tailored for rural India use cases in areas such as agriculture smart farming solutions to invest in IoT infrastructure in rural and remote regions.

   c. **Skill Development Programs:** Implement skill development programs to train local workforce on IoT technologies and applications.

   d. **Regulatory Frameworks:** Establish clear and supportive regulatory frameworks for IoT deployment in rural areas, to address issues such as device interoperability & standardization, data privacy, and security.

   e. **Awareness & Inclusive Access Programs:** Conduct awareness campaigns to educate citizens, businesses, and local governments implement programs to ensure inclusive access to IoT-enabled services, focusing on affordability and accessibility for all citizens.

f. **Incubation Centers and Innovation Hubs:** Establish incubation centres of excellence and innovation hubs in rural areas to support local entrepreneurs and start-ups to develop IoT solutions.

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?

VIL Comments to Q.5

1. It is crucial to spread awareness about IoT enabled smart applications to ensure that the citizens understand the benefits and potential of these technologies. Governments can take various initiatives to raise awareness and promote the adoption of IoT, some of such key initiatives are listed below:

   a. **Educational Campaigns:** Launch comprehensive educational campaigns through various media channels, including television, radio, print, and online platforms to explain what IoT is and how it can benefit citizens. Conduct webinars, online courses, and provide downloadable resources to reach a wider audience, especially in urban and remote areas.

   b. **Community Workshops and Training Programs:** Organize workshops and training programs at the community level to provide hands-on experience with IoT devices and applications.

   c. **Partnerships with Educational Institutions:** Collaborate with schools, colleges, and universities to integrate IoT-related topics into the curriculum and conduct awareness programs.

   d. **Demonstration Projects:** Implement IoT demonstration projects in public spaces, such as smart parks, intelligent street lighting, or connected public transportation systems to showcase the tangible benefits of IoT.

   e. **Mobile Apps and Interactive Platforms:** Develop mobile applications and interactive online platforms that provide information, tutorials, and updates on IoT technologies.

   f. **Inclusive Communication:** Ensure that communication materials are inclusive and in local language, considering linguistic and cultural diversity to reach all segments of the population along with a robust feedback mechanism to understand citizens' concerns, questions, and suggestions related to IoT.

2. In addition to above, engaging private companies and start-ups in developing IoT applications is also crucial for the success of awareness initiatives. It is required to incentivize their participation for more effective and innovative awareness campaigns due to the following reasons:

   a. **Expertise and Innovation:** Private companies and startups often possess expertise in technology and communication strategies, which contribute towards innovative and effective approaches to raise awareness campaigns.

b. **Resource Mobilization:** Private companies can bring financial and technical resources to the awareness initiatives, helping in the development and execution of comprehensive campaigns.

c. **Industry Credibility:** Involving private companies lends added weight to awareness campaigns, as their involvement signifies industry support and validation.

d. **Customized Solutions:** Private companies and start-ups may develop customized solutions for awareness campaigns, aligning them with the preferences and behaviors of specific target audiences.

e. **Market Opportunities:** Incentivizing private companies can create market opportunities, encouraging them to develop innovative products and services that cater to the needs of an informed consumer base.

3. Further, following incentivization approaches can also be considered:

a. **Grants and Subsidies:** Offer financial grants, subsidies and tax benefits to private companies and start-ups engaged in developing and executing IoT projects.

b. **Recognition and Awards:** Establish awards/recognition programmes to acknowledge private companies and start-ups that demonstrate excellence in implementing unique projects that brings benefits to the society. Organize work stream and forums where private companies, startups, and government officials can collaborate, share best practices, and explore partnership opportunities.

c. **Access to Government Resources**: Provide private companies with access to government resources, such as research data or communication channels, to enhance the effectiveness of their campaigns.

d. **Capacity Building Programs**: Develop capacity building programs that enhance the skills and capabilities of private companies, enabling them to contribute more effectively to awareness campaigns.

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.

VIL Comments to Q.6.

1. Upskilling the top management and owners of industries is vital to ensure that they understand and leverage the opportunities presented by Industry 4.0, which includes artificial intelligence,

robotics, Big Data, and IoT. Following are some of the Suggested measures for upskilling the top management and owners of industries:

a. **Customized & Executive Training Programmes:** Develop customized technology immersion training programmes that address the specific needs and challenges faced by top management in their respective industries. Encourage top management to enroll in executive/digital education programmes offered by reputed institutions specializing in Industry 4.0 technologies.

b. **Cross-Functional Workshops:** Organize cross-functional workshops that bring together leaders from different departments to foster collaboration and a holistic understanding of Industry 4.0.

c. **Industry-Specific Seminars and Conferences:** Facilitate participation in industry-specific seminars and conferences focused on the applications of AI, robotics, Big Data, and IoT.

d. **Case Studies and Best Practices Sharing:** Share case studies and best practices from companies which have successfully implemented Industry 4.0 technologies.

e. **Risk Management Training:** Provide training on risk management associated with Industry 4.0 implementation, including cybersecurity and data privacy considerations.

2. Upskilling the workforce is also as important as upskilling the top management and owners of industries in the era of Industry 4.0, where technologies like artificial intelligence, robotics, big data, and the Internet of Things (IoT) are changing the nature of jobs. Following are some of the measures which can be adopted to upskill the workforce in industries:

   a. **Identify Skills Gaps:** Conduct comprehensive skill gap analysis to identify the current capabilities of the workforce. Design and implement training programs that are tailored to the specific needs of the workforce, focusing on the skills required for Industry 4.0.

   b. **Digital Literacy Training:** Provide basic digital literacy training to ensure that all employees have a foundational understanding of digital technologies. Invest in online learning platforms that offer variety of courses on relevant Industry 4.0 technologies.

   c. **Cross-Functional Training:** Implement cross-functional training programs to encourage employees to develop skills beyond their immediate job roles. Conduct hands-on workshops and simulations to provide practical experience with Industry 4.0 technologies.

   d. **Certification Programs:** Support employees in obtaining relevant certifications for Industry 4.0 technologies. Collaborate with universities and technical schools to offer specialized courses or degree programs related to Industry 4.0.

   e. **Employee Feedback Mechanism:** Establish a feedback mechanism to understand employees' training needs, preferences, and challenges.

3. To adopt these upskilling tasks, collaborative efforts between government entities, private companies, and educational institutions are the key requisites. Following are some public-private partnerships which can be adopted for the upskilling needs associated with Industry 4.0:

a. **Industry-Academia Collaboration:** Encourage partnerships between industries and academic institutions to design and deliver upskilling programs. In terms of global best practices, we would like to submit that Germany's dual education system is an exemplary model where companies collaborate with vocational schools to provide hands-on training and education. This system ensures a direct link between education and industry requirements.

b. **Joint Funding Initiatives:** Create joint funding initiatives where both public and private sectors contribute to the financing of upskilling programs. Singapore's Skills Future initiative involves joint funding from the government, employers, and individuals. Employers contribute to the Skills Future Enterprise Credit, which supports workforce training and upskilling.

c. **Digital Innovation Hubs:** Establish digital innovation hubs that serve as collaborative spaces for public institutions, private companies, and research organizations to jointly develop and deliver upskilling programs. For eg. The European Union's concept of Digital Innovation Hubs promote collaboration between industry and research organizations to facilitate the digital transformation of businesses. These hubs offer a platform for joint innovation and skill development.

d. **Government-Industry Skill Councils:** Establish skill councils that bring together government agencies, industry associations, and private companies to identify skill gaps, design training programs, and facilitate their implementation. Our country's National Skill Development Corporation (NSDC) collaborates with various sector skill councils to develop industry-relevant skill standards and certification programs. Private sector involvement further ensures alignment with market demands.

e. **Tax Incentives for Private Sector Participation:** Provide tax incentives to private companies investing in upskilling initiatives, encouraging their active participation just like the United Kingdom's Apprenticeship Levy which requires large employers to invest in apprenticeship training. This approach encourages companies to actively participate in upskilling their workforce.

f. **Sector-Specific Training Consortia:** Form training consortia within specific industry sectors, bringing together multiple companies to collectively address the upskilling needs of their workforce. For e.g. the Manufacturing Institute in the United States works with manufacturers to establish sector-specific training consortia. This collaborative approach ensures that upskilling efforts align with the unique needs of the manufacturing sector.

Q.7. What are the policy, regulatory and other challenges faced by MSMEs in India 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.

VIL Comments to Q.7

1. MSMEs are backbone of the Indian economy. By making MSMEs stronger digitally, it would be easier for the country to become 5 trillion dollar economy. However, MSMEs in India face various

challenges in adoption of Industry 4.0, some of which are listed below along with the Suggested measures to resolve the same:

Sl. No.	Topic	Regulatory & Policy Challenges	Suggested Measures that may be adopted by the Government
1.	**Standardization, Interoperability and Data Security**	▪ Legacy systems that are difficult to communicate with. ▪ Lack of standardized protocols for interoperability and data security/ privacy hinder the seamless integration of Industry 4.0 solutions. ▪ Inadequate digital & network infrastructure is a significant obstacle for MSMEs.	▪ Prioritize development of digital infrastructure, including high-speed internet and reliable power supply, in key industrial zones. ▪ Introduce regulations mandating adherence (including specification of norms in Government RFPs/tenders) to standardized protocols that ensure data protection and privacy compliance for Industry 4.0 technologies. ▪ Introduce certification programmes for MSMEs to demonstrate compliance with data security standards.
2.	**Investment and ROI Constraints**	MSMEs often face these constraints on investments that limit their ability to invest in expensive Industry 4.0 technologies.	▪ Introduce financial incentives, tax breaks, or subsidies to reduce the financial burden on MSMEs adopting Industry 4.0. ▪ Facilitate partnerships between the Government and industry to create funding mechanisms or low-interest loans for MSMEs.
3.	**Skill Gaps**	Shortage of skilled labor with expertise in Industry 4.0 technologies.	▪ Develop and fund skill development programmes specifically tailored for MSMEs. ▪ Encourage partnerships between MSMEs, educational institutions, and technology providers to create specialized training programs.
4.	**Collaboration and Networking**	These opportunities are essential for MSMEs to learn from each other and share best practices.	▪ Establish regulatory sandboxes where MSMEs can test and implement Industry 4.0 solutions in a controlled environment. ▪ Conduct regular consultations with industry stakeholders to update regulations in line with technological advancements.

2. In addition to the above, best practices in other countries are also provided below:

   a. **Germany:** Mittelstand 4.0 Competence Centers: Germany has established competence centers that provide SMEs with information, training, and support for the implementation of Industry 4.0 technologies.

b. **Singapore:** SMEs Go Digital Program: Singapore's Government has a comprehensive program that provides funding support, guidance, and incentives to help SMEs adopt digital technologies, including Industry 4.0 solutions.

c. **South Korea:** Smart Factory Initiative: South Korea has implemented a Smart Factory initiative that supports SMEs in adopting smart manufacturing technologies through funding, training, and infrastructure development.

d. **United Kingdom:** Made Smarter Program: The UK's Made Smarter initiative offers support to SMEs for adopting digital technologies, including the development of skills, access to funding, and technology adoption advice.

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.

VIL Comments to Q.8.

1. Strengthening the National Trust Centre (NTC) framework for comprehensive security testing and certification of IoT devices, including both hardware and software, under DoT/TEC involves a multi-faceted approach.

2. In our view, following are some of the additional measures which can lead to enhancement of the NTC framework:

   a. **Alignment with International Standards:** Align the NTC framework with internationally recognized security standards for IoT devices.

   b. **Security by Design Principles:** Incorporate security by design principles into the NTC framework, emphasizing secure development practices throughout the IoT device lifecycle.

   c. **Periodic Review and Update:** Establish a periodic review mechanism to update the NTC framework in response to evolving cybersecurity threats and technological advancements. Introduce provisions for third-party security audits to complement the NTC's certification process.

   d. **Cross-Sector Collaboration:** Facilitate collaboration between the NTC and other regulatory bodies, industry associations, and cybersecurity experts to gather diverse perspectives and expertise.

   e. **Continuous Monitoring of Certified Devices:** Implement a continuous monitoring mechanism for certified IoT devices post-deployment, with the ability to revoke certifications if security vulnerabilities are identified.

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?

VIL Comments to Q.9.

1. IoT security challenges and requirements vary significantly across different industry verticals. Due to this, we believe that along with common stated policy principles, additional sector-specific IoT security and privacy guidelines can be beneficial. Some such reasons to affirm the same are provided below:

    a. **Different Risk Profiles:** For eg., Healthcare devices require strict compliance with patient privacy laws, whereas industrial IoT devices might prioritize physical safety and operational continuity**.**

    b. **Regulatory Compliance:** Various sectors are subject to different regulations. Developing guidelines that are tailored to meet specific regulatory requirements can help organizations ensure compliance more efficiently.

    c. **Varied Data Sensitivity:** The type of data collected and processed can range from relatively innocuous environmental telemetry to highly sensitive personal or financial information, necessitating different levels of security.

    d. **Diverse Operational Environments:** IoT devices in a factory setting face different threats compared to those in a smart home or within a connected vehicle. Sector-specific guidelines can address these environmental variables effectively**.**

    e. **Legacy Systems Integration:** Many industries have legacy systems with which IoT devices must integrate. Tailored security guidelines can help address the unique challenges of securing such integrations.

2. Further, we would like to submit that sector-specific IoT security and privacy guidelines, in this regard, should be developed in consultation with all stakeholders.

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.

VIL Comments to Q.10.

1. As mentioned in our response to Q.9, since IoT security challenges and requirements vary significantly across different industry verticals, sector-specific IoT security and privacy guidelines can be beneficial.

2. However, to develop such sector-specific guidelines, a common framework and methodology are needed to ascertain the following:

a. **Interoperability:** With IoT devices often interacting across different sectors, a common framework can facilitate interoperability and secure communication between devices from different industries.

b. **Uniformity in Core Principles**: A common framework ensures that all sector-specific guidelines adhere to a set of fundamental security principles, providing a baseline of protection across the board.

c. **Efficiency in Development**: It allows for the efficient creation of new guidelines as new sectors adopt IoT technologies, by providing a template that can be customized rather than starting from scratch each time.

d. **Compliance and Assessment**: A unified approach can streamline compliance checks and security assessments, making it easier for businesses and regulators to ensure that the guidelines are being followed.

e. **Adaptability to Emerging Threats**: A common framework can be regularly updated to reflect emerging threats, providing a dynamic approach to security that can be quickly adopted by various 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.

VIL Comments to Q.11.

1. The Digital Personal Data Protection Act, 2023 provides the following safeguards:

   a. **Obligations of Data Fiduciaries:** to implement technical and organizational measures to ensure data protection, including data breach notification protocols.

   b. **Protection of Children's Data:** with provisions like verifiable parental consent for data processing and restrictions on tracking and behavioral monitoring.

   c. **Additional obligations on Significant Data Fiduciaries**: Identified based on the volume and sensitivity of data processed to comply with additional obligations like appointing a Data Protection Officer and conducting Data Protection Impact Assessments.

   d. **Rights of Data Principals**: including the right to access, correct, update, and erase their data, and ensure these rights are facilitated by Data Fiduciaries.

   e. **International Data Transfer: Allow** international data transfers to countries with adequate privacy protections, ensuring data is only shared with entities that provide a similar level of data protection.

   f. **Enforcement Powers:** Data Protection Board can enforce the Act, conduct inquiries, issue directions, and impose penalties for non-compliance.

g. **Conflict with Other Laws**: provisions of the Act shall prevail in case of any conflict with other existing laws, to maintain consistency in data protection norms, except in cases where stricter rules are applicable.

h. **Rule-making Powers**: granted to the Central Government to facilitate the implementation of the Act and to address emerging data protection challenges.

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.

VIL Comments to Q.12.

1. To encourage research and development of IoT use cases in various sectors, we believe that following policy and regulatory measures can be considered:

   a. **R&D Tax Credits and Deductions**: Offer tax credits or deductions for expenses related to R&D in IoT. This could include costs associated with prototyping, testing, and personnel.

   b. **Government Grants and Subsidies**: Provide direct funding opportunities for projects that demonstrate potential for significant advancements in IoT technology.

   c. **Education and Training Programs:** Invest in education programs to create a skilled workforce capable of developing and implementing IoT solutions.

   d. **Standardization and Interoperability:** Develop and promote industry standards to ensure interoperability and security of IoT devices, encouraging wider adoption.

2. In addition to above, incentivization of startups should be considered for research and development of IoT enabled use cases in various industry verticals incentives for startups. These incentives can stimulate innovation, economic growth, and the adoption of advanced technologies. Here are some measures to incentivize start-ups in this domain:

   a. **Seed Funding for IoT Startups**: Create dedicated funds to provide seed capital to startups working on IoT in sectors like healthcare, agriculture, and smart cities. Also, encourage the formation of venture capital funds that specialize in IoT by offering them tax breaks or co-investment opportunities.

   b. **Matching Grant Programs:** Implement programmes where Government matches, dollar for dollar, the R&D investments made by private entities in IoT.

   c. **Market Access and Export Assistance:** Assist startups in accessing domestic and international markets, including compliance with global standards and export facilitation.

d. **Discounted Access to Technology:** Negotiate with technology providers to offer cloud services, analytics platforms, and other necessary tools at discounted rates to eligible startups.

Q.13. What measures should be taken to encourage centres of excellence to handhold startups working in the development of use cases and applications in 5G and beyond technologies? How can the domestic and foreign investors be encouraged to invest for funding the startups for these kinds of development activities?

VIL Comments to Q.13.

1. To encourage centres of excellence (CoE) to handhold startups working in the development of use cases and applications in 5G and beyond, several measures can be taken which are listed below:

    a. Facilitate partnerships between CoE and private companies. These collaborations can provide startups with access to expertise, technology and capital.

    b. Offer grants, subsidies, or tax incentives to CoE that provide significant support to startups in 5G technologies. This could cover costs related to mentorship, access to labs, and technology licensing.

    c. Develop specialized incubation programs within CoE that focus on 5G technology, offering workspace, technology access, mentorship, and business development support.

    d. Provide CoE with the resources to create state-of-the-art testing and demonstration facilities for startups to trial and showcase their 5G solutions.

    e. Establish regulatory sandboxes that allow startups to test new 5G applications and business models without the normal regulatory constraints.

    f. Support programs within CoE that focus on skill development in 5G technologies, ensuring startups have access to a talented workforce.

2. Further, the domestic and foreign investors can be encouraged in following ways to invest for funding the startups for these kinds of development activities:

    a. Offer tax benefits to investors who put capital into startups and innovation in the 5G domain.

    b. Create government-led investment funds that match private investments in startups working on 5G technologies to reduce investor risk.

    c. Develop clear and stable regulatory frameworks for 5G applications to reduce investor uncertainty.

    d. Foster international collaboration between domestic startups and leading global 5G firms to increase credibility and attract foreign investment.

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

VIL Comments to Q.14

1. In our view, there is a need to revisit and possibly update relevant laws to address various issues, including liability regimes and effective mechanisms for redressal and compensation in the context of emerging technologies like IoT, drones, and robotic systems. These technologies introduce new challenges and complexities, and adapting legal frameworks is essential to ensure responsible use and accountability. Some suggestions in this regard are provided below:

    a. **Liability Frameworks:**

        i. Establish strict liability regimes for manufacturers and operators of autonomous systems where they are held liable for damages without the need to prove negligence. Develop models that apportion liability among all parties involved, including manufacturers, software developers, and users.

        ii. Require mandatory insurance coverage for operators and manufacturers of drones and robotic systems to ensure compensation for damages.

    b. **Cybersecurity:**

        i. Introduce mandatory cybersecurity standards for IoT devices to prevent unauthorized access and use.

        ii. Oblige companies to report security breaches involving IoT and autonomous systems to authorities and affected individuals in a timely manner.

    c. **Airspace and Operational Regulations for Drones**:

        i. Develop laws for low-altitude airspace management to prevent collisions and ensure the safe operation of drones.

        ii. Clearly define no-fly zones and operational restrictions for drones to protect sensitive areas and ensure public safety.

    d. **Robotic Systems**:

        i. Establish ethical guidelines for the development and use of robotic systems, particularly those involving AI decision-making.

        ii. Mandate human oversight for decisions made by autonomous systems where there is a significant impact on individuals or the public.

    e. **Redressal and Compensation Mechanisms**:

i. Set up specialized fast-track courts or dispute resolution mechanisms for cases involving IoT, drones, and robotics.

ii. Create funds specifically allocated for compensating victims of accidents caused by these technologies.

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.

VIL Comments to Q.15.

1. Multi-access Edge Computing (MEC) introduces additional complexities to the security landscape due to its distributed and edge-centric architecture. While MEC inherits many security principles from traditional cloud computing, the unique characteristics of edge environments necessitate specific considerations. Following are some inputs and suggestions regarding policies, rules, regulations, and guidelines for implementing a secure MEC framework:

   a. **Access Control:**

      i. Mandate the use of strong authentication protocols for devices and users accessing MEC services.

      ii. Implement RBAC policies to limit access to MEC resources based on user roles and responsibilities.

   b. **Standardization and Compliance:**

      i. Develop and enforce industry-wide security standards specific to MEC deployments, possibly through standard-setting organizations like ETSI or IEEE.

      ii. Create a compliance certification process for MEC providers, ensuring adherence to established security standards.

   c. **Physical Security:**

      i. Establish guidelines for the physical security of MEC nodes, including protection from unauthorized access and environmental hazards.

      ii. Ensure the integrity of hardware and software components through secure supply chain practices.

   d. **Edge Device Security:**

      i. Introduce security standards for IoT devices that connect to MEC infrastructure to prevent them from becoming attack vectors.

ii. Mandate secure boot mechanisms and regular firmware updates for devices interacting with MEC networks.

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?

VIL Comments to Q.16

1. The Metaverse together with enabling technologies like AI, Web3, Block-chain and high speed connectivity with new generation technologies would certainly enhance use cases within gaming, education, e-commerce, manufacturing, and virtual real estate, creating new business prospects and revenue streams across industries worldwide. The extensive capability of Metaverse to create immersive and life-like experiences for user or customer by using wearables and walkthrough programs is all set to reach 7 billion US$ by 2026 within gaming market in terms of app downloads making India the world's largest mobile gaming markets.

2. The rural and remote areas of India would benefit from the diverse applications and use cases such as language agnostic education programs to support over 122 recognized languages and 780 dialects aided by 2D/3D visualization thereby generating increased level of student engagement in offline, online, hybrid learning environments and enabling personalization of learning.

3. In India, where 46% of its population is under age 25, the Digital skill empowerment within rural and semi urban areas can fuel the growth of the metaverse. Such skilling will act as a key enabler to provide rural and urban youth the much needed skills to understand and develop programs within gaming, entertainment and hospitality industry by building entertainment platforms such as gaming and films. It could make the metaverse more accessible to many who already engage with these platforms not only within India, but globally as well. The Indian media conglomerate has already started benefitting out of it, i.e. Zee Entertainment etc. welcomed its recruits via the metaverse for the first time and also plans to introduce NFTs from TV shows, movies, music, and original web series and so on.

4. Metaverse applications and use cases built around hotels & restaurants industry can provide virtual reality tours or options to explore their hotel with an avatar during the booking process. This allows guests to get a clear sense of what to expect before they commit to booking a hotel room or through virtual reality technology, cutting-edge restaurants can provide the tools for customers to fully explore their menu before booking, including options to see how a meal is prepared, or to check out the facilities.

5. Additionally, integration of the secure and seamless digital transactions like USSD, UPI, and AEPS will propel India's Metaverse economy further so that these developed Indian mobile apps can be subscribed & monetized remotely from any part of globe.

6. Hence, to create awareness and promote use of Metaverse amongst the citizens, including those residing in rural and remote areas, the main requisites are building the awareness and skilling up of the individuals. It is only through that they can benefit from the diverse Metaverse use cases

and services. Proper trainings and accessibility to required ecosystem along with handset subsidies and connectivity will help the individuals create new economic activities and increase employment opportunities thereby promoting economic growth of the country.

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, especially when users may have multiple digital identities and avatars across different platforms and jurisdictions?

VIL Comments to Q.17

1. The regulatory and the cybersecurity policies will be critical to govern metaverse especially looking at its advances in creating digital twins and avatars using augmented reality (AR), virtual reality (VR), and 3D environments, having potential to create identical vision/looks, speech/voice and various gestures. All this topped up with artificial intelligence (AI) and machine learning can be easily misrepresented globally.

2. Further, as the Metaverse is an innovative technology which has the potential to transform the way we interact with each other and our surroundings, therefore activities such as data collection, surveillance and use of AI and machine learning can all put user data and privacy at risk.

3. All the above requires simultaneous implementation of activities like putting up data protection regulations in place, security of AR/VR devices, and awareness amongst the users regarding the potential risks and related protective measures. The upcoming digital regulatory framework i.e. the Digital India Act (DIA) for the metaverse applications related misinformation and misrepresentation needs to be strengthened both technologically and awareness wise with respect to detection of frauds, curb crimes or incite violence, etc.

4. The protection of data pertaining to personal information can be achieved in multipronged ways. Users can be made aware that they can use pseudonyms or avatars to protect their identity, or by using privacy-enhancing technologies such as encryption, secured communication protocols, virtual private networks (VPNs), or differential AI/Machine Learning homomorphic privacy techniques. These technologies can help to obscure or anonymize user data, making it more difficult for third parties to track or identify individuals.

5. Further, protection of user from cyberattacks, harassment and manipulation in the metaverse can be attained in multiple ways like avoiding malicious downloads, infected virtual objects, or compromised content that can install malware on their devices or virtual environments. Also, use of reputable virtual marketplaces and platforms that have security measures, being vigilant and skeptical of unsolicited messages, requests, or offers within the metaverse, installation of latest security patches and updates regularly, usage of strong, unique passwords and enablement of two-factor authentication (2FA) or multi-factor authentication (MFA) can also aid protection from cyberattacks.

6. In addition to above, it is also necessary to be cautious of granting unnecessary permissions to third-party applications or services, avoiding executing files or scripts from untrusted sources that could trigger a ransomware attack, regular updating of the VR or AR headset firmware and software provided by manufacturers that often release updates that address security vulnerabilities and improve overall device security. One should also avoid connecting VR or AR headsets to public Wi-Fi networks and use trusted and secure networks like virtual private network (VPN) to encrypt network traffic and protect one's privacy.

7. Apart from all the above measures, Metaverse platforms and applications must also be regularly embedded with robust security measures to protect user data from unauthorized access, breaches, or cyberattacks by employing techniques including end-to-end encryption, data-at-rest encryption, differential privacy, homomorphic encryption, and secure multi-party computation to safeguard user privacy etc. Block-chain-based credentialization services and metaverse versions of multifactor authentication and multi-signature verifications must be considered.

8. When it comes to data transmitted between IoT devices and the Metaverse, data needs to be secured. Thus, use of encryption and access controls and implementation of secure communication protocols such as HTTPS or MQTT with authentication especially for the companies creating content can be done.

9. Also, it is expected that identity theft and fraud will be major risks in the metaverse given the prevalence of digital identities, avatars, and virtual assets. To mitigate such ricks, implementation of multifactor authentication and other identity verification techniques such as biometric recognition, knowledge-based authentication and one-time passwords in metaverse application development can be used to help secure virtual identities against unauthorized access.

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.

VIL Comments to Q.18.

1. It is expected that metaverse has the potential to generate up to 5 trillion US$ in value by 2030. In fact a large scale organization like Facebook, changed their brand name to Meta in order to reflect the company's ambition to become a metaverse company. While companies such as Microsoft, Nvidia and Google are planning to launch their own virtual worlds or infrastructure for building the metaverse, brands ranging from Nike to HSBC are sharing their plans to launch a virtual world presence or selling NFTs. Looking at these trends being followed by the large multinational companies, massive outsourcing of products and services is expected globally.

2. In addition to above, the Government of India has announced PLI scheme for 13 sectors to create national manufacturing champions and generate employment opportunities with total outlay of INR 1,97,291 crores. The PLI scheme for mobile devices now needs to be extended to the entire hardware space catering to the AR/VR headsets, industrial cameras, sensors and the paraphernalia which cater to the metaverse ecosystem. These export opportunities emanating

from the IT/ITeS MNCs and start-ups will help propel India to achieve a 20 per cent digital economy by 2025.

3. Both Central & State Governments in India are taking significant steps to promote metaverse & related advanced technologies including AI, Big Data, Cloud, Web-3.0, Block-chain etc. States organizations such as Tamil Nadu Start-up and Innovation Mission (TANSIM) has set up an ambitious target to establish approximately 10,000 start-ups in Tamil Nadu by 2026.

4. Similarly, from educational and skilling perspective, organizations such as Meta, are collaborating with 15 universities across the US who are actively embracing immersive learning including Stanford University.

5. Hence, looking at all such enormous opportunities, it becomes imperative for start-ups, innovators and researchers to collaborate to capitalize the opportunity by establishing experimental campuses where all of them can collaborate and develop or demonstrate technological capabilities, innovative use cases, and operational models for Metaverse.

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 effective and significant contribution in Metaverse standardisation? Kindly provide elaborate justifications in support of your response.

VIL Comments to Q.19.

1. Metaverse is an evolving technology which can support digital initiative for better, secured and efficient services access to customers with desired satisfaction. The process of Metaverse services and practice improvement plan will help regulate the metaverse with respect to potential social and economic issues looking at the massive amount of investment projected for the same. Standardization is imperative to maintain the balance between optimizing metaverse services to users and ensuring that regulations protect the potential profits of investors over their large investments.

2. India being the largest democracy in the world, has large stake in Metaverse, both as consumer as well as service provider, as compared to other countries across the world. Therefore, standardization organizations like Metaverse India Policy and Standards (MIPS), a forum specific for Metaverse standards and policy in India, along with CAVE IIT Madras in association with a cluster of international standards agencies and many others will help build a pervasive, open, and inclusive metaverse on a global scale, simultaneously supporting India socially and economically.

3. Globally, Metaverse Standard Forums (MSF) and its working group on standards is responsible for the development of standards and use case registers. The Standards Register Working Group is developing the above products using various web tools such as GitHub and Google Forms and bespoke implementations of other tools. Some of the key tasks that need to be addressed by these forums and organizations include creating a control body, build optimal user experience, outreach, glossary for standardized configuration and the use cases management.

4. Especially, initiatives supported by Metaverse Standards Register (MSR), the publicly-accessible, searchable register of all Pre-qualified Organizations and Groups (POGs) and any standards-

related publications and projects (SPPs) will create relevant Metaverse interoperability, apart from having formal and informal standards organizations to regulate emerging, completed and adopted standards, standardization projects, specifications, guidelines, or open source projects etc.

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.
(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.

VIL Comments to Q.20

1. The appropriate governance mechanism for a thriving virtual universe is imperative for sustainable growth within digital India as well as across globe. Such governance is very important as it represents a collective virtual space where users can engage, interact, and transact with one another in real time. Within this interconnected digital world, novel challenges arise, which necessitate the development of robust governance mechanisms. In our view, the concerns around metaverse governance would mainly revolve around the following:

    a. **Virtual Economies:** As in the metaverse, virtual currencies and assets especially bitcoins, cryptocurrency etc. hold tangible value, leading to the emergence of virtual economies, these economies require governance to prevent frauds, and money laundering, and ensure fair and transparent transactions. Establishing mechanisms for virtual asset ownership, value stability, and economic regulation will be crucial.

    b. **Regulatory Frameworks:** As the metaverse grows, questions surrounding jurisdiction and regulatory oversight become increasingly complex. Balancing individual freedom and user rights with the need for regulation to protect against illicit activities, such as cybercrime and infringement of intellectual property, pose a significant challenge. It will be essential to develop global standards that consider cultural, legal, and ethical nuances.

    c. **User Rights and Protection:** With an increasing number of people engaging in the metaverse, it becomes imperative to safeguard user rights. Issues related to privacy, data protection, content moderation, and digital identity management need careful consideration. Striking the right balance between empowering users and ensuring their safety within virtual environments require thoughtful governance frameworks.

2. The above mentioned concerns make it essential to put forth potential frameworks in order to govern Metaverse in a better manner. The same can be done with the following methods:

    a. **Decentralized Governance:** Embracing decentralized models, such as block-chain technology, can offer transparency, immutability, and user empowerment. Smart contracts and decentralized autonomous organizations (DAOs) can enable peer-to-peer governance, allowing users to collectively make decisions and shape the rules and policies of metaverse.

b. **Cross-Sector Collaboration:** Metaverse governance should involve collaboration between technology companies, Government, regulators and user communities. Establishing consortiums, industry standards bodies, and multi-stakeholder platforms can foster dialogue, encourage information sharing, and facilitate the development of inclusive and effective governance frameworks.

c. **Ethical Guidelines and Auditing:** The metaverse should adopt ethical guidelines, emphasizing inclusivity, diversity, and accessibility. Regular audits and third-party certifications can ensure compliance with these guidelines, promoting responsible practices and mitigating risks associated with discriminatory or harmful content.

d. **User-centric Design and Feedback:** User feedback and involvement should be at the core of metaverse governance. The platforms must provide mechanisms for users to report issues, propose changes, and participate in decision-making processes. User-elected representatives can amplify the voices of the community and contribute to the formulation of policies.

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?

VIL Comments to Q.21.

1. Metaverse is an evolving technology and in order to address the key concerns and risks, the regulatory framework is a key to facilitate safeguarding of the digital experience of users as well as promotion of business for enterprises.

2. The regulatory and the cybersecurity policies will be critical to govern metaverse especially looking at its advances in creating digital twins and avatars using Augmented Reality (AR), Virtual Reality (VR), and 3D environments, having potential to create identical vision/looks, speech/voice and various gestures topped up with Artificial intelligence (AI) and machine learning can be easily misrepresented globally.

3. Metaverse users can become victims of many real world frauds as transactions would often use cryptocurrencies, which currently do not have Government-backed fraud protection standards and additional services in the metaverse can be sold as non-fungible tokens (NFTs), which are digital assets with non-tangible values that can be fraudulently manipulated.

4. As risk analysis for Metaverse applications and innovations, the companies must consider scenario modeling to identify new risks and mitigation strategies and then communicate them to users and regulators to build awareness especially in dealing with issues like bullying, harassment, stalking, grooming, and hate speech that may manifest in metaverse environments using various branches of AI like speech recognition, Natural Language Processing (NLP), computer vision and reinforcement learning.

5. India certainly requires regulatory body well in-line with international bodies such as Federal Trade Commission (FTC) which is the main regulatory body overlooking the metaverse to enforce marketing and competition law on the Internet.

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?

VIL Comments to Q.22.

1. The User-Generated Content comes in the usual form of text, voice, images and videos, all of which present challenges for moderating the speed. Due to the advancement in technologies, fast, customizable solutions are available now, and today's moderation tools are accurate at scale, and largely up to the task. The metaverse, however, has introduced new challenges for brands which are aligned to ensure the safety of users.

2. Image Moderation, Video Moderation, Speech Moderation and Text Moderation are the primary four types of Moderation Services for Metaverse. In real time, all these formats can be transcribed and translated into meaningful intents & conceptuality. In video content moderation objects, people, unsuitable material (such as pornography), alerts, warning signals and even words (if it's a handwritten sign) may all be detected by image moderation.

3. While image moderation comes in handy when you wish to moderate an existing database of photographs. On the other hand, Image and video content moderation is ineffective for picture moderation since it does not allow you to exclude certain items from the picture frame.

4. Virtual reality systems in Metaverse work by capturing extensive biological data about a user's body, including pupil dilation, eye movement, facial expressions, skin temperature, and emotional responses to stimuli. Spending just 20 minutes in a VR simulation leaves nearly 2 million unique recordings of body language. This denotes massive data acquisition and advanced analytics complexities from inference viewpoint.

5. Moreover, existing data protection frameworks are woefully inadequate to deal with the privacy implications of these technologies. Data collection is involuntary and continuous, rendering the notion of consent almost impossible. The research also shows that five minutes of VR data, with all personally identifiable information stripped, could be correctly identified using a machine learning algorithm with 95% accuracy. This type of data isn't covered by most biometrics laws.

6. Big Tech and its investors are betting heavily on the metaverse because they want people to spend even more time online so that they can then collect more data, which ultimately, can be sold to advertisers. This model of "surveillance capitalism" will be unimaginably deepened with biometric data from virtual reality worlds, adding to the massive amounts of user data already extracted and harnessed by tech companies.

7. A survey of users of popular VR headsets showed that 49% of female and 36% of male respondents reported experiencing some form of sexual harassment. Automated facial recognition and predictive analytics with artificial intelligence (AI) are already being used by law enforcement authorities in many parts of the world, often in the absence of data protection laws exposing metaverse users to greater risk.

8. The need is to regulate and limit the personal, data-driven economy and bring it under lenses strictly before extended reality technologies become normalized among younger users.

9. It is therefore, critical for all the stakeholders participating in Metaverse services, especially the user, vendor and regulatory and governance bodies to collaborate and coordinate on content moderation through an automated feedback reinforcement modeling approach.

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.

VIL Comments to Q.23.

No comments.

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.

VIL Comments to Q.24.

1. India, being the world's most populous country, the National Digitization is not only the need but necessity for the growth of economy and better user experience, thereby, contributing to global Digital economy and growth. Therefore, 5G, IoT and Metaverse technologies, topped up with AI based use cases are all set to play a critical role as enablers to the growth of nation as well as the world and digital transformations.

2. To support promotion of the development, deployment and adoption of 5G use cases, our Hon'ble Prime Minister awarded 100 '5G Use Case Labs' to the educational institutions across the country. The institutions will get 5G Use Case Labs as part of the DoT initiative to ensure relevant use cases are identified and deployed in India with global standards.

3. Leveraging the capabilities of 5G, which has increased transmission speed and network capacity, and reduced latency in association with IoT, Metaverse with AI technologies, has huge potential for various industries including healthcare, education, entertainment, industrial IoT/manufacturing, autonomous vehicles and smart Cities. Some such use cases are listed below:

    a. Manufacturing Use Cases with IIoT sensors and robotic machines include:
        i. Preventive maintenance through IIoT sensors.
        ii. Productivity and performance monitoring.
        iii. Providing internet connectivity to legacy machines without replacement.
        iv. Controlling robotics remotely with no noticeable delay or interference.

b. Healthcare Use Cases include:
   i. Inventory management of machines, drugs, supplies, and medical waste.
   ii. Physical location tracking of life-saving equipment.
   iii. Preventive maintenance sensors that automatically create work orders.
   iv. Secure cross-campus service for both staff and patients.

c. Autonomous Vehicle based 5G Use Cases include:
   i. Automatic updates, security patches, and feature additions.
   ii. Real-time weather, traffic, and safety updates to vehicles in route.
   iii. Safe retrieval of stolen vehicles.

d. Education based 5G Use Cases include:
   i. Providing controlled internet access for students at home.
   ii. Designing reliable cellular blanket coverage across campus.
   iii. Using IoT sensors to track classroom attendance, study room availability, and public transportation.
   iv. Securely segment staff and students networks.
   v. Promote fast and reliable outdoor learning.

e. Smart City based 5G use cases include:
   i. Fleet tracking.
   ii. Infrastructure monitoring with IoT sensors.
   iii. City-wide video surveillance and traffic cameras.
   iv. Secure and controlled internet access for residents.

f. Transportation 5G applications are:
   i. Fleet tracking.
   ii. Automatic time-stamping of shipped and received products.
   iii. Dynamic insights based on live data.
   iv. Highly accurate inventory management and capacity planning.

g. Entertainment applications are:
   i. Proactive maintenance via IoT sensors.
   ii. Secure and reliable guest access through neutral host services.
   iii. Ensuring both indoor and outdoor areas have high-speed network access.
   iv. Providing reliable service to a large unpredictable number of devices.

x---------- End of Document ----------x