Jio DIGITAL LIFE

RJIL/TRAI/2023-24/264
26th December 2023

To,
Ms. Vandana Sethi,
Advisor (Admin)
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawaharlal Nehru Marg, New Delhi - 110002

Subject: **RJIL's comments on TRAI's Consultation Paper on "Digital Transformation through 5G Ecosystem".**

Dear Sir,

Please find enclosed the comments of Reliance Jio Infocomm Limited (RJIL) on the Consultation Paper dated 29.09.2023 on **"Digital Transformation through 5G Ecosystem"**.

Thanking you,

Yours Sincerely,
For **Reliance Jio Infocomm Limited**

KAPOOR SINGH GULIANI

Digitally signed by KAPOOR SINGH GULIANI
Date: 2023.12.26 16:59:46 +05'30'

Kapoor Singh Guliani
Authorized Signatory

Enclosure: As above

Reliance Jio Infocomm Ltd

Reliance Jio Infocomm Limited’s comments on TRAI’s Consultation on “Digital Transformation through 5G Ecosystem”

Preface:

1. Reliance Jio Infocomm Limited (RJIL) thanks the Authority for giving an opportunity to offer comments on the important consultation paper on **Digital Transformation through 5G Ecosystem.**

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

3. **5G applications or 5G triangle comprising of eMBB (Enhanced Mobile Broadband), mMTC (Massive Machine Type Communications) and uRLLC (Ultra-Reliable and Low Latency Communications) are poised to revolutionize all sectors of economy.**

4. The impact will not only be seen in innovations but also in streamline processes and operations and delivering new age customer experiences. The low latency associated with 5G will deliver real-time communication and propel the use of Extender Reality (ER) including augmented reality (AR) and virtual reality (VR) along with Artificial Intelligence (AI) and Machine learning (ML).

5. 5G capacities and its ecosystem will help enable new business models and revenue streams by supporting newer generations of applications and use cases that were not possible before. This will be a boon for Internet of Things (IoT), Industry 4.0, autonomous vehicles, smart cities, smart monitoring of manufacturing processes, robotics, automation, and AI driven smart factories.

6. In this context, it is important to delve upon the need to identify any requirement of policy changes or new policy framework that will foster better and faster adoption and effective utilisation of new technologies for the holistic and sustainable development of the economy driven by 5G ecosystem.

7. We understand that the Authority and the Government are already seized of these issues and a lot of efforts have already been made to ensure that Indian companies and citizens get the maximum benefit out of this generational transformation under 5G ecosystems.

8. All concerned ministries and departments are involved in identifying and promoting India specific 5G use cases in different industry verticals like Healthcare, Education, Governance, Banking, Finance, Insurance, Cyber Security, Enterprise transformation, Industry 4.0, Agriculture, Livestock, Smart Cities & Infrastructure and many more. There is massive scale of cross functional collaboration already happening, however, it can be said that it would further benefit by providing an open platform to bring private sectors and innovators together, along with the public sector.

9. We understand that **major area that India needs to focus on is adequate and defining participation in the development of standards pertaining to 5G ecosystem, associated devices and global policies.** There is a need for devising measures to increase awareness about 5G, its use case, robotics, AI&ML, Internet of Things (IoT), Metaverse and its benefits as well as risks in rural and remote parts of the country.

10. The Authority and Government have already created a robust licensing/regulatory mechanism in the country for communication services and associated sectors under the Unified License framework and TRAI Act. Further the personal data of Indian customers is protected under the Digital Personal Data Protection Act 2023 (DPDP Act). The MeitY under its various legal requirements governs the digital content in its various aspects.

11. In this background, we believe that it will be premature to go for more regulations and controls, especially when 5G ecosystem and its use cases in various industries; Metaverse and its applications etc. are still evolving and need all the freedom to innovate and deliver beneficial outcomes. It is worthwhile to mention here that even globally the approach has been to support for growth and observe new developments. Therefore, the Authority is requested to continue with its policy of light touch regulation and continued monitoring developments to ensure that any market failure is averted.

12. One aspect where regulatory simplification is required is IoT or Machine to Machine (M2M) communications. These services are already being used extensively in some sectors however, this specialized communication is overburdened with restrictive regulatory requirements and there is a need to create a collaborative regulatory regime for this, post addressing the concerns of stakeholders.

Issue wise response:

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.

RJIL Response:

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

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

3. Another aspect of the cross-sector collaboration is the industries collaborating directly on mutually agreed terms for development and adoption of 5G use cases. The global examples clearly show that the initiatives in this direction have to be taken by the industries themselves, be it the 5G providers collaborating with OEMs or the first movers in Industry 4.0 collaborating with carriers.

4. While there is no scope for regulatory intervention to improve or strengthen the collaboration. Following facilitative features can be helpful in bringing the industries together.

5. **Collaborative Platform:** The Government can institutionalize an open, independent and non-obtrusive interactive platform like a chat platform that brings together all the interested parties i.e., TSPs, generational transformation professionals from Industries like, healthcare, manufacturing and education, and all other relevant areas on one platform. The collaborations can organically emerge on meeting of minds. In order to further facilitate or increase adoption of this platform, some basic goals and objectives directed towards objective outcome can also be prescribed.

6. Regular interaction between stakeholders on this platform can lead to sharing of insights to better each other's efforts. Whenever required, this can progressively turn into

formation of working groups and task forces that can devote energies to overcome different challenges. This will also help identify common issues and share solutions.

7. **Participation in Standards:** The Government should ensure that Indian Industry has sufficient representative participation in global standard making bodies. This will help ensure that our emerging use cases conform with the evolving global common standards for 5G applications across sectors. This in turn will facilitate interoperability and seamless integration.

8. **Public-Private collaborations:** Government should encourage more and more public sector enterprises and Government departments to collaborate with private companies on equal footing to develop and implement 5G use cases, for instance the ongoing development of use cases by ministry of Housing and Urban development for smart cities ; smart grid and smart meter use cases by Ministry of Power, measures to expand the role of ICTs to further expand the New Education Policy etc. .

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.

RJIL Response:

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

2. The most critical part for this is the availability and allocation of spectrum. Dense 5G implementation will require massive amount of spectrum. In addition to all the already auctioned spectrum bands and plans to auction E-Band and V-Band spectrum, the Authority should also plan to auction 6 GHz band, full C-Band and 28 GHz band (on flexible use basis). We submit that all IMT identified and IMT targeted spectrum should be made available to TSPs. Further all available spectrum should be auctioned on regular basis. This should be supplemented by a clear policy position against delicensing of spectrum to quell the regular noise.

3. The Regulatory framework should become more agile to incorporate emerging 5G related requirements. There is a need for definitive action to address regulations around EMF and restrictive Net Neutrality and data charging Rules. The Authority should recommend for adoption of ICNIRP norms for EMF. Further, there is a need to upgrade the regulatory

framework for new use cases. Recently Ofcom carried out a review[1] of Net Neutrality, some of the excerpts from the statement are as below:

"Our *review has found that, in general, it has worked well and supported consumer choice as well as enabling content providers to deliver their content and services to consumers. However, there are specific areas where we provide more clarity in our guidance to enable ISPs to innovate and manage their networks more efficiently, to improve consumer outcome.*

- ***ISPs can offer premium quality retail offers:*** *Allowing ISPs to provide premium quality retail packages means they can better meet some consumers' needs. For example, people who use high quality virtual reality applications may want to buy a premium quality service, while users who mainly stream and browse the internet can buy a cheaper package. Our updated guidance clarifies that ISPs can offer premium packages, for example offering low latency, as long as they are sufficiently clear to customers about what they can expect from the services they buy.*

- ***ISPs can develop new 'specialised services':*** *New 5G and full fibre networks offer the opportunity for ISPs to innovate and develop their services. Our updated guidance clarifies when they can provide 'specialised services' to deliver specific content and applications that need to be optimised, which might include real time communications, virtual reality and driverless vehicles.*

- ***ISPs can use traffic management measures to manage their networks:*** *Traffic management can be used by ISPs on their networks, so that a good quality of service is maintained for consumers. Our updated guidance clarifies when and how ISPs can use traffic management, including the different approaches they can take and how they can distinguish between different categories of traffic based on their technical requirements.*

- ***Most zero-rating offers will be allowed:*** *Zero-rating is where the data used by certain websites or apps is not counted towards a customer's overall data allowance. Our updated guidance clarifies that we will generally allow these offers, while setting out the limited circumstances where we might have concerns.*

We also clarify that we are unlikely to have concerns where ISPs take reasonable approaches to provide services with clear public benefit. This includes enabling ISPs to prioritise and zero-rate access to emergency services, offer parental controls, manage internet traffic on transport and in public spaces where there is limited capacity available,

[1] https://www.ofcom.org.uk/consultations-and-statements/category-1/net-neutrality-review

and prevent access to scam websites and other harmful content. Finally, we set out our views on the possibility of allowing ISPs to charge content providers for carrying traffic, which might lead to more efficient use of networks. While there are potential benefits to a charging regime, we have not yet seen sufficient evidence that this is needed and believe there is enough flexibility provided for ISPs in our other proposals. Ultimately whether or not a charging regime should be introduced in the UK is a decision for Government and Parliament. Since leaving the EU we have not needed to take account of European guidance, although it has remained part of our approach to net neutrality. We have decided to replace this guidance in its entirety and have now produced a single, comprehensive set of guidance."

4. **Infrastructure Support**: While the Government has come out with multiple facilitative policies and measures, a lot remains to be done to smoothen the approval processes and reduce the fees with regards to ROW, permissions for use of street furniture for small cell and aerial fiber deployment etc.

5. **Sunset date for legacy technologies:** The Government should come out with a policy and glidepath for closing down the 2G and 3G networks completely so that unnecessary network costs should be avoided, and all customers can be migrated to 4G and 5G services. This will also give great impetus to developing ecosystem to 5G use cases.

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?

RJIL Response:

1. We do not think much effort is required to create awareness of 5G in urban areas and many of the rural areas. However, there is a need to create awareness of 5G use cases in many rural areas. However, more than policy measures this will require creating communication strategies that speak to the targeted audience.

2. This will require association with the local government bodies, schools and other community organizations, banks, agricultural cooperatives, and relevant government agencies and to use their communication networks to proliferate knowledge of 5G. Notwithstanding the above, the real deal breaker would be 5G only killer apps that can organically become viral in rural areas. Of course, content in local languages will also play the role of a catalyst.

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?

RJIL Response:

1. IoT or M2M communication have been here for a while and many regulatory policies have been developed to streamline the operations and foster innovation in this field. The industry has also represented to the Government, many times, to address the restrictive features of the regulations governing these services to increase their adaptability. We submit that addressing these issues is equally important for proliferation of IOT services in rural areas. A few of these issues are reproduced here for ready reference.

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

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

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

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

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

iii. **Point of Sale (PoS):** The modern-day POS machines provide multiple services like payments via all types of digital modes, recharges, e-payments like traffic challans etc. and connecting with GST application among other activities from a single interface device, making the 4 IP restriction completely unviable.

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

B. Standardization/certification of IoT/M2M device

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

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

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

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

8. We have already provided our detail submission on this issue vide our comments to the consultation paper on "Embedded SIM for M2M Communications" dated 25th July 2022. We submit that there is a need for uniform policy **for integration of Subscription Manager Secure Routing (SM-SR) platform for all the M2M devices being imported in the country.** Currently many devices being imported are equipped with eSIM with a bootstrap profile

which is registered on company's own SM-SR platform based out of India. **Therefore, for facilitating download of Indian TSP's profile into these eSIM, SM-SR change is required through integration between these two SM-SR as per GSMA guidelines.**

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

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

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

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

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

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

D. Exemption for M2M SIMs from Data barring orders

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

16. We submit that is as IoT/M2M applications cover critical areas such as manufacturing, telemedicine & healthcare, connected vehicles, home equipment, smart meters etc., these should not be covered under the data services shut down orders issued by the Government authorities. **It is pertinent that as these SIMs comply with restrictive communication requirements, they cannot be used for any anti-social activities and can easily be excluded for data services shutdown requirements.**

E. Industry body for facilitating and strengthen the IoT/M2M ecosystem.

17. The Authority has already taken lead in recommending consultative industry body for areas of coordination for cloud services and Traffic management practices etc. We submit that the nascent stage of ecosystem development in M2M services warrants that a similar body comprising of all stakeholders should be recommended for development of IoT/M2M ecosystem as well.

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

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

G. Permit availability of eSIM from outside India

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

H. Integrated SIMs

20. The **integrated SIM (ISIM) technology is very cost-effective and a boon for low power M2M devices that have multiple usage, especially in remote areas.** We submit that this technology should be facilitated and ISIM personalization may be permitted from outside India as this implementation is tightly integrated with modem chipset**. However, in order to ensure network integrity, compliance with the structure and security guidelines issued by 3GPP and GSMA respectively should be mandatory for ISIM.**

I. Default URLs to be allowed in M2M offering.

21. We submit that for M2M application, there are many default URLs (i.e., google APIs, GPS accuracy, DNS, Device Management URLs, firmware upgrade, remote SIM management etc.) connectivity to which is imperative for effective services. **We submit that there should be no restriction on connectivity with these urls and it should be made available on default basis as these URLs will not carry any customer or application specific data but will only help in delivering better services and management.** Some of these urls are as below:
    i. DNS – for url resolution
    ii. Network Time Protocol (NTP) service like time.google.com, in.pool.ntp.org etc.
    iii. Assisted GPS (AGPS) Services - Example Qualcomm XTRA Service: (xtra[1-3].gpsonextra.net, xtrapath[1-3].izatcloud.net) etc.
    iv. Google APIs – googleapi.google.com used for API Discovery Service

J. Allowing single profile for AIS 140 solution

22. The present AIS140 guidelines by MORTH mandating minimum 2 profiles from different operators to ensure connectivity to device are not relevant in view of ubiquitous coverage offered by TSPs across India. **Therefore, such mandate should be relaxed and single MNO profile under AIS 140 should be permitted.**

K. Regulations on Custodian update in case of ownership change

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

Q.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?

RJIL Response:

As mentioned in the previous response, there is not much effort required to create awareness of IOT in urban areas and many of the rural areas, as smart meters and other IOT applications have already reached many rural parts of the country. Further, aforementioned policy measures are required to facilitate the proliferation of these services. Needless to add that real adoption will come from benefits being propagated through word of mouth.

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.

RJIL Response:

1. The important step is to take measures for upskilling the workforce for IOT. This will involve education, understanding and training to absorb the necessary skillsets for designing, developing, deploying, and managing IoT technologies. This can be done through a combination of targeted training programs and initiating appropriate small and long duration courses and programs in educational institutes. Another measure can be to prepare the training module in association with IOT industry players, device vendors and solution providers to create customized training modules.

2. We understand that major upskilling efforts will have to be taken by the industries involved in IOT or planning to leverage the same and there can be no distinction of public or non-public industries in this scenario. All industries will have to get involved to create suitable training modules.

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.

RJIL Response:

1. We submit that one of the major challenges faced by MSMEs in India is the lack of Digital inclusion of MSMEs, as highlighted by the Authority in another Consultation Paper. Addressing that would be the first step in increasing the adoption of Industry 4.0 by the MSMSs. In response to consultation paper on "Digital Inclusion in the Era of Emerging Technologies" we have submitted **adopting the German example of creating enhanced Competence Centres to assist the MSMEs become digital.** These centres can also be leveraged to train the MSMEs in adopting Industry 4.0.

2. The Government is already having a major focus on MSMEs, and many steps have been taken to improve the productivity and skillsets of MSMEs. CHAMPIONS (Creation and Harmonious Application of Modern Processes for Increasing the Output and National Strength) portal and Ministry of MSMEs through its control rooms is providing every possible support on a local level to MSMEs in the areas including finance, market access, technology upgradation, skill development etc. and training and adapting to IOT and Industry 4.0 should also be made part of these efforts, without need for a new policy initiative.

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.
And
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?
And
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.

RJIL Response:

1. As note by the Authority, its proposals on security measures for IOT devices and National Trust Centre under recommendations on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine Communications", of September 2017, have been accepted by the Government. Further, the "Framework of National Trust Centre for

M2M/IoT Devices and Applications (TEC 31188:2022) R1.0" released by TEC in March 2022, provides for STQC (Standardization Testing and Quality Certification) under MeitY (Ministry of Electronics and Information Technology) as the agency to carry out such testing under single window of proposed National Trust Centre".

2. The testing and Certification of IoT devices hardware is already covered in Essential Requirements (ERs) under Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) with testing specifications related to EMC, Safety, communication interfaces, IP, SAR and Security. Thus, under the present framework, IoT device hardware is to be tested as per Essential requirement (ER) prepared by TEC, and the software by STQC.

3. This is in addition to various specific and general requirements and guidelines like "Code of practice for securing Consumer IoT" to ensure an ecosystem of secured devices and reducing vulnerabilities. Evidently, the regulatory framework is already in place to address trust related issues and challenges if any pertain to effective implementation of this framework.

4. We understand the Authority's concern for lack of sector specific focus on addressing the digital risk element, however, understand that once the IOT deployment crosses the nascent stage, the sectoral regulators would take appropriate action on this. Further, this issue is better discussed at inter-regulator forums.

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.

RJIL Response:

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

Q.12. What additional policy and regulatory measures are required to encourage research and development of IoT use cases in various sectors? Is there a need to incentivize startups for research and development of IoT enabled use cases in various industry verticals? If yes, kindly suggest measures for the same.

And

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?

RJIL Response:

1. It is important to provide special fiscal incentives for increased spending on R&D by Startups in all fields including IOT. We should follow the global examples of redesigning R&D tax incentives to make them more effective for budding entrepreneurs. The funding programs should be for the entire innovation lifecycle (Ideation, POC, Prototype, Commercialization). This will help overcome the final barrier of commercializing the inventions.

2. The Government has already set up a dedicated program under the "Startup India", under the Department for Industrial Policy and Promotion (DPIIT) to provide a platform for connecting with mentors and to improve learning by means of online courses for entrepreneurs to develop business and technology skills, and a Startup guidebook. This mission can be extended to provide support at research and development of IoT enabled use cases in various industry verticals level that will eventually translate to Start-ups.

3. The Government can also explore the possibilities of tying up with global research institutions for developing research mindset and setting up research labs and skill development centres across the country to ensure a harmonious growth in research ecosystem.

4. The private sector investment can also be in the form of grants, aids, setting up school level laboratories, Start up support and collaboration with academia. All these activities should be considered for tax-breaks.

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.

RJIL Response:

We believe that there exists a clear allocation of roles and responsibilities among the various stakeholders involved in IoT like internet providers, device manufacturers to app service providers among others. Therefore, we are not entirely sure that there is a need to create liability regimes for IoT at this stage and how and why the present laws will not be sufficient to address the challenges. While a specific and effective mechanism for redressal and compensation for damages caused by IoT devices or applications may seem desirable at ideation stage, there needs to be practical world justification for such a change, if at all the laws are to be changed, which is not clear from the Consultation Paper.

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.

RJIL Response:

1. As noted by the Authority, edge computing comes with its inbuilt data privacy related solutions where all the data is processed inside the country and there exists a legal process to ensure that such sensitive data is handled as per the legal provision under DPDP Act and IT Act.

2. We understand the concern regarding lower security standards or capabilities of the Ede computing devices than centralized cloud servers, however, with the implementation of DPDP Act, the data controllers and fiduciaries are legally bound to process and store the data in a secure manner and there does not seem to be any need for a separate security mechanism for Multi- access Edge Computing (MEC).

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?

RJIL Response:

1. We agree with the Authority that metaverse is not a distant or hypothetical concept and India needs to be at forefront of the generational transformational through Metaverse. We understand that on a higher level there is awareness of Metaverse. However, there can be many awareness measures that can be used to create an enthusiasm in the young engineers and students to help the country grab this unique opportunity to shape and benefit from this emerging phenomenon.

2. Holistic and comprehensive focus on Metaverse will help unleash the forces that will help India leverage its strengths in information technology, innovation, and creativity and address the issues pertaining to quality education, health care and employment opportunities in farthest and far-most areas of the country.

3. We suggest following measures for promoting awareness of metaverse.

    a. **Leveraging Social-Media**- Many of the popular social media platforms already delve into Metaverse and enable the user to create their own avatars. These mediums should be leveraged to increase awareness of Metaverse. Services of influencers, especially those in local languages should be used.

    b. **Education System**: The educational institutes should be involved in promoting the awareness of Metaverse by including this as part of curriculum.

    c. **Awareness meets:** The Government should leverage power of Indian coding and technical communities by creating events like Hackathons, metaverse based seminars and webinars, live demonstrations, and experiments.

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?

RJIL Response:

1. There is no doubt that Metaverse will lead to increased exposure of consumer's personal data through increased virtual interactions. This can potentially lead to a surge in threats of data breaches, however, it will be wrong to state that we do not have dedicated data protection legislation post promulgation of DPDP Act, to address such issues. The vigorous implementation of the Act will ensure that the users are able to trust the content and services they access in the metaverse.

2. While we believe that it is apt time to develop a regulatory framework for the responsible development and use of Metaverse, however, it will be better to have a multi-regulator body to tackle the issue regarding jurisdiction first.

3. These regulatory efforts should be supported by awareness efforts to ensure that Indian consumers control their personal information and identity in the metaverse. They should be made aware of the possible and known cyberattacks, harassment and manipulation in

the metaverse. The awareness measures suggested in the previous section can be simultaneously used to spread awareness about these risks and challenges with Metaverse.

4. There remain valid concerns on ensuring the data privacy and security in the metaverse, especially when users may have multiple digital identities and avatars across different platforms and jurisdictions, however, regulating these aspects has to be a gradual evolving process and dedicated rules can be framed as we learn more about the use cases and potential threats.

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.

RJIL Response:

1. We agree with the Authority that for orderly growth of an innovative technology like Metaverse, there is a need to provide a conducive environment for testing and validating new technologies and applications. Establishment of experimental campuses where startups, innovators, and researchers can collaborate and develop or demonstrate technological capabilities, innovative use cases, and operational models for Metaverse will be an important step in this direction.

2. The Centre of Excellence (CoE) for IoT (MeitY, NASSCOM, ERNET initiative) under the Digital India Initiative has been useful in strengthening the start-ups ecosystem. The capacities and capabilities of these COEs can be a good starting point for the experimental campuses. This will help foster cross-disciplinary and cross-sectoral collaboration among all stakeholders in the development and adoption of the 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.

RJIL Response:

1. We agree with the Authority that there is a need to prevent monopolization of the Metaverse by ensuring development of open Metaverse standards. These protocols and

standards will help keep the metaverse open for all and will foster innovation, collaboration, and inclusion in the metaverse ecosystem.

2. India should participate in all global standardization efforts starting with ITU-T Focus Group on metaverse (FG-MV). We should ensure that interoperability protocols are deployed at all various levels. This will enable different metaverse platforms and applications to communicate and interact with each other seamlessly.

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.

RJIL Response:

There is a need for new paradigm in governance due to the decentralized nature of Metaverse. As mentioned in previous sections this will require collaborative legal and regulatory approach. We understand that a thorough examination of emerging concepts like Mirror governance and global trends will be required to settle the governance model for Metaverse. However, at current nascent stage a policy of light touch regulation and Forbearance may be important to foster innovation. Further, national level mechanism would be more relevant, supported by a global level understanding.

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?
And
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?

RJIL Response:

We submit that there are many contours to content moderation in the metaverse and globally this field is deemed to be still in an evolving stage. This is a complex and evolving field that requires careful consideration at various levels before taking a firm position. The MIT Technology Review article shared by of the Authority itself indicates that there are no settled principle, and the Big Tech is using its own standards to govern the content. This already complex situation is further complicated by the fact that on a regulator level the governance will need to be done of cross-border content with no legal jurisdiction. We understand that in the beginning the content moderation practices and rules by MeitY should continue to prevail and we build onto this base, as more knowledge is available.

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.

RJIL Response:

We do not think that it is an appropriate stage to modify the legal framework with regards to IPR at this nascent stage of metaverse development. The prevailing IPR framework should be simplified and made conducive for R&D professionals and that should suffice for metaverse as well.

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.

RJIL Response: None