Bharti Airtel Ltd.
India & South Asia
Airtel Center, Plot No. 16,
Udyog Vihar, Phase - IV,
Gurugram - 122 015
Haryana, India

www.airtel.in
Call +91 124 4222222
Fax +91 124 4243252

TRAI/FY24-25/37
Dated: 19.08.2024

To,
Shri Akhilesh Kumar Trivedi,
Advisor (Network, Spectrum and Licensing)
Telecom Regulatory Authority of India,
World Trade Centre,
Nauroji Nagar
New Delhi – 110 029.

Subject: Response to Consultation Paper on "Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs"

Dear Sir,

This is in reference to TRAI's Consultation Paper on the "Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs" 24.06.2024 (6/2024)

In this regard, please find enclosed our counter comments for your kind consideration.

Thanking You,

Yours' Sincerely,
For **Bharti Airtel Limited**

Rahul Vatts
Chief Regulatory Officer

Encl: a.a

Preamble:

At the outset, Airtel would like to thank the Authority for issuing this important consultation paper entitled, "*Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs.*"

The adoption of Machine to Machine (M2M) communications and Internet of Things (IoT) has significantly transformed the landscape of critical infrastructures across industries from energy grids to transportation systems, water supply networks to transportation systems and many many more. The seamless connectivity they bring has increased efficiency and automation, convenience and innovation. In India, industrial IoT in 2023[1] dominated the market with a projected market volume of US$9.67 bn with IoT market revenues reaching US$27.31 bn.

N**etwork connectivity, importantly, is the fundamental component** of the overall technical solution for such large-scale, critical infrastructure deployment projects. Smart metering is one example of such a project. The interconnected networks of devices, systems, platforms and applications work together to enable seamless communication, data exchange, automation and analytics. They involve a variety of components that collaborate to collect, process, analyse and act upon data from the physical world.

Government initiatives like '***Digital India***', '***Smart Cities Mission***' and regulatory policies like '***National Digital Communications Policy***' as well as the issuance of **M2M Service Provider Guidelines** and the **13-digit numbering series for M2M services** have played an important part in accelerating M2M/IoT deployment and improving efficiencies and economies.

As India proceeds with its ambitious rollout plan for such interconnected critical infrastructure (e.g., smart grids and meters), cyber vulnerabilities also continue to rise. There are growing threats of cyberattacks on critical infrastructure like power grids and remote healthcare. Additionally, **there are increasing numbers of large-scale, low-powered, wide area networks (LPWANs) being deployed by unlicensed operators over unlicensed spectrum bands**. This usage of unlicensed bands is putting confidentiality, integrity, availability, reliability and accountability of such critical **public infrastructure at serious risk**.

In the highly interconnected world of the devices and systems of M2M/IoT, mitigating all risk to security is a collective responsibility and such threats **need to be addressed by one and all, equally.** Licensed Telecom Service Providers (TSPs) follow such an approach. Telecom is considered amongst the most critical of all infrastructure from the perspective of National Security and is deployed on the principles of zero trust, accordingly, with each network component undergoing rigorous testing and approvals.

[1] Internet of Things - India | Statista Market Forecast

The **National Security Directive on the Telecommunications Sector (NSDTS)** approved by the Government takes all such holistic aspects into consideration. Today, licensed TSPs, ISPs, NLDOs, ILDOs and even the captive network license holders (CNPNs) all follow the approach of 'Trusted Products' obtained from 'Trusted Sources' which then go into their networks.

However, that is not yet the case with unlicensed operators operating in unlicensed bands who, despite offering the same service to the same customers including in critical sectors, are not subject to the same non-negotiable security norms as applicable to licensed operators towards communications networks, services and devices.

Moreover, license-exempt bands not governed by 3GPP or any such standardisation body, and because the technologies are proprietary, are also not interoperable. In the event of any disruption, such a standardisation, harmonisation and interoperability gap would further adversely impact the public at large.

Airtel wishes to highlight that recognising the importance of such critical segments/sectors for the purposes of M2M/IoT very early, the Authority, in its Recommendations dated 05.09.2017 on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications"[2], had recommended that "…*Government, through DoT, should identify critical services in M2M sector and these services should be mandated to be provided only by connectivity providers using licensed spectrum*".

The recommendation was accepted by DoT and an Inter-Ministerial Working Group (IMWG) was formed in November 2019 to deliberate on all issues concerning critical M2M services. The IMWG in its report in March 2021 recommended a list of 20 services[3] to be classified as critical along with broad regulatory requirements for critical services.

However, there has not been much progress since. This is where the timeliness and importance of the present consultation paper comes in. The present consultation paper should now move the needle on the issue of security of deployment of M2M/IoT for critical services. The Authority in its 2017 recommendations aptly enunciated the requirement of operating critical services in licensed spectrum (*e.g., exclusive rights in terms of usage, shielded for any interference, measurable and enforceable QoS parameters, and government having administrative control over the licensed connectivity providers, and ability of telecom networks to be able to prioritise the carriage of information on their network based on the critical nature of information*).

In Airtel's considered view, such deployments should not only be done using the licensed spectrum, but security and related measures should also be applied equally to every participant so that the rules of the game are clearly defined.

[2] https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf
[3] The list of 20 services is reproduced by the Authority at para 2.16 of the instant Consultation Paper under discussion

Response to CP on *Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs*

Summary:

- ✓ *A guiding regulatory framework should be created that defines critical M2M/IoT services. This framework should be consistent across industries so as to be able to facilitate wide coverage and efficient resource allocation.*

- ✓ *A criterion should be created to classify services as critical, i.e,*
  - *Services which support critical business services and infrastructure of important national interest*
  - *Services whose disruption can lead to grave consequences such as disruption of public utility services*
  - *Services whose disruption can cause health, safety and environmental hazards to citizens.*

- ✓ *To level the playing field, mitigate security as well as service outage risks; and to protect the interests of the exchequer and public at large, the critical M2M/IoT services should be provided using licensed spectrum bands.*

- ✓ *All M2M devices to be used for critical M2M/IoT services in India should be brought under the NSDTS framework.*

- ✓ *A regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs should be established. It should cover scenarios such as M&As, hive off/split, takeover of companies, Transfer of Ownership from parent to subsidiaries/other group companies or vice versa, or between the subsidiaries/group companies of a single parent, cessation of operations or filing for bankruptcy by M2MSP, Change of System Integrators (SI) by principal entities.*

- ✓ *The transfer of ownership should also be allowed between inter-circle and intra-circle entities.*

A detailed response to the consultation paper is provided in the subsequent sections.

Q1. Whether there is a need for a broad guiding framework for defining a service as critical M2M/IoT service? If yes, what should be the guiding framework? Please provide a detailed response with justifications.

Airtel Response:

Yes, there is an urgent need to create a guiding framework for defining a service as critical M2M/IoT service. The framework should be consistent across industries, facilitate wide coverage and efficient resource allocation. The need for such a framework was also part of the TRAI Recommendations[4] in 2021 and the IMWG report in March 2021.

Airtel requests that the regulatory framework should be created at the earliest since TRAI had made its recommendations in 2018 and as an industry, we are still deliberating the finality of the issue in 2024. In the meanwhile, lakhs of IoT devices have been installed in critical infrastructure by unlicensed operators but without the same levels of security standards as those being imposed on licensed TSPs.

Criteria for Definition of Critical M2M/IoT Services:

DoT, in its reference to the Authority preceding the instant Consultation Paper, has suggested that "*Criticality in any sector may be use-case driven and the same may not be made applicable for the entire domain/ sector. The criticality of M2M services in any domain/ sector may be decided on the market requirement by concerned ministries on their own. …*".

However, segregating various use cases in a particular sector into critical and non-critical could end up being a very tedious and cumbersome exercise and may lead to inconsistencies and gaps in areas of national security and public safety. Thus, a more uniform and holistic approach needs to be adopted by TRAI and DoT.

Therefore, it is Airtel's submission that the framework for defining critical M2M/IoT services should consider the importance of such services vis-à-vis the network, security and public at large. Accordingly, **the following broad classifications under which critical M2M/IoT services should be considered:**

i. Services which support critical business services and infrastructure which is of important national interest
ii. Services whose disruption can lead to serious consequences such as disruption of public utility services and loss of revenue to Government
iii. Services whose disruption can cause health, safety & environmental hazards to citizens.

[4] Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications, https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf

This approach will also align with the national critical information infrastructure intent.

Consistent with the above criteria, the TRAI Recommendations and the IMWG Report of 2021, the following definition for critical services in the M2M/IoT sector should be considered:

> ***"Critical Services in the M2M/IoT sectors are services involving time-critical applications that are extremely sensitive from an economic, strategic and public impact perspective, and hence require the secure delivery of information within a specified duration with requisite reliability and QoS. The devices and equipment involved in such services should be able to achieve very low latency, ultra-reliability, always-on connectivity along with carrier/Telco grade security. These services will require robust, resilient, reliable, redundant and secure networks and should only be provided using licensed spectrum and the devices involved should be compliant with the Trusted Products and Trusted Sources framework (National Security Directive on Telecommunication Sector – NSDTS)".***

Based on the above, the segments to be included in the list of critical M2M/IoT services can be *energy smart grids; defence networks; mission critical remote surgery and other health related applications; safety & surveillance; state, commercial and home security monitoring; surveillance applications, fire alarm, police among others.*

An indicative but detailed list of critical M2M/IoT services (including the services already approved by IMWG) is provided in *Annexure-A.*

In view of the above, Airtel recommends:

1. **Framework for critical M2M/IoT services should be defined.**
2. **NSDTS framework should be applied on the devices used for critical M2M/IoT services.**

Q2. Through the recommendation No. 5.1(g) of the TRAI's recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017, TRAI had recommended that critical services in the M2M sector should be mandated to be provided only by connectivity providers using licensed spectrum. Whether this recommendation requires a review? Specifically, whether critical services in the M2M sector should be permitted to be provided by using unlicensed spectrum as well? Please provide a detailed response with justifications.

Airtel Response:

No, there is no need to review the TRAI recommendation that critical services in the M2M sector should be mandated to be provided only by connectivity providers using licensed spectrum.

While making this recommendation in 2017, the TRAI provided its reasoning, reiterated below:

"*2.46 M2M services and applications can be differentiated based on its nature as critical and non-critical. A large number of devices and applications in M2M/ IoT ecosystem will be non-critical in nature. These devices may be either connected through Personal Area Network (PAN) to a local gateway or there may be SIM based standalone connectivity using cellular network. However, there would be some critical M2M applications that would require robust, resilient, reliable, redundant and secure network. For example, M2M applications in healthcare like remote surgery or a driverless car etc. These kinds of applications require high QoS, ultra reliability, very low latency, very high availability and accountability. If there is any variation in QoS, latency or availability, it can cause substantial damage to customers. It is pertinent that such throughput and latency sensitive application should run only on robust wired optical fiber, copper network or LTE capable access networks.*

2.47 As stated earlier, operation in licensed spectrum has certain exclusive rights in terms of usage and is also shielded for any interference. Also, the QoS parameters are measurable and enforceable. Moreover, the government has administrative control over the licensed connectivity providers. So, critical services should be identified and mandated to be provided by connectivity provider using licensed spectrum. Hence there is a need to identify critical services in which, quality of service, if deficient, could result in serious consequences. Also, the telecom networks should be able to differentiate the critical services from the non-critical services and prioritize the carriage of information on their network based on the critical nature of information…"

As evident, the TRAI recommendation was made after duly considering multiple inputs provided by stakeholders and the realities of the M2M/IoT ecosystem. **Nothing has changed since then**. **Hence, critical services in the M2M sector should be provided only by connectivity providers using licensed spectrum.**

In fact, the importance of the security of communications networks and services has only increased manifold over the years. The government has come up with various new security norms — a majority of which are applied on the licensed TSPs as soon as they acquire licensed spectrum under the Unified License (with access service authorisation).

However, the unlicensed players using unlicensed spectrum continue to remain outside the ambit of any such regulatory oversight.

The concern of security risks cannot be sidestepped by considering aspects of SLAs and QoS between two entities. Indeed, the issue of licensed spectrum versus unlicensed spectrum is not so much an issue of QoS and SLA, but rather beyond that, i.e., about end-to-end secured network for which licensed operators make huge investments into network and information security.

Both these aspects (SLAs and QoS), while important in isolation, cannot address the risks to security of communications networks and services. The licensed TSPs acquiring licensed spectrum are obligated to ensure security measures in parallel. It is not an either-or situation.

Therefore, in the matter of the security of communications network and services, there cannot be two yardsticks for judging two entities offering the same service in the very same market. Maintaining such a regulatory lacuna will only cause increased vulnerability to threat and risks in the case of unlicensed operators and pose serious risks of disruption in critical public services/ infrastructure such as Public Utility Services.

The security conditions for the connectivity / communications network and service should work as a baseline for all participants, and any SLA conditions should continue to be an independent requirement by the user entity.

The licensees already comply with the frameworks of the National Security Directive on the Telecommunications Sector (**"NSDTS"**), the Mandatory Testing and Certification of the Telecommunication Equipment (**"MTCTE"**). Further, the Telecom Security Operations Centre (**TSOC**) of DoT continuously monitors and mitigates any cyber security crisis in the telecom sector. These security measures only further enhance confidence and trust in the ecosystem. The same should be applicable to the unlicensed operators.

The gravity of this issue can be understood from an example — today, various state DISCOMs have been rapidly issuing tenders for smart metering projects with approximately 222 million smart meters already sanctioned[5]. Out of these, a total of 118mn have been awarded to Advanced Metering Infrastructure Service Providers ("AMISPs). As per industry estimates, a significant number of deployments are being done by unlicensed operators using licence-exempt bands, and these projects involve lakhs of meters across cities or even states.

Now, since there are no common baseline security requirements for such unlicensed networks, there is no testing and monitoring and no mandatory equipment deployment under **trusted sources framework**, this makes it easier for threat actors to obtain central access to the control centre as well as the databases required for operating the smart grid and causing potential disruption in the entire ecosystem.

In view of the above facts, Airtel recommends that:

1. **In order to mitigate and address security threats and service outage risks, to protect the interests of the exchequer as well as the public at large, the critical M2M/IoT services should be provided by connectivity providers using licensed spectrum bands.**

[5] https://www.nsgm.gov.in/en/sm-stats-all

Q3. Whether there is a need to bring M2M devices under the Trusted Source/Trusted Product framework? If yes, which of the following devices should be brought under the Trusted Source/Trusted Product framework:

(a) All M2M devices to be used in India; or
(b) All M2M devices to be used for critical IoT/M2M services in India; or
(c) Any other (please specify)?

Please provide a detailed response with justifications.

Airtel Response:

Yes, the M2M devices for critical M2M/IoT services should be brought under the Trusted Source/Trusted Product framework.

Telecom is among the most critical sectors in terms of infrastructure from the perspective of National Security and is deployed on the principles of zero trust. This is why each network component undergoes rigorous testing. All devices and equipment purchased by licensed TSPs to integrate into their networks must be certified as 'Trusted Products' obtained from 'Trusted Sources' as part of their compliance with NSDTS. In fact, TSPs comply with the NSDTS requirement even with respect to communication devices which operate using unlicensed spectrum – such as Wi-Fi routers, as well as devices which do not even use spectrum – like GPON, PRI gateways, etc. **However, in the case of unlicensed operators such as the AMISPs operating on unlicensed bands, their Data Concentration Units (DCUs), which are also tightly coupled with Network Interface Cards (NIC), do not come under any such framework**.

It may be noted that in addition to various Unified License (Access services authorisation), CMTS/UASL holders, there are many other license holders, for example, as of 31st May 2024:

- 1897 ISP Authorisations under Unified License[6]
- 735 ISP Authorisations under UL-VNO[7]
- 44 ISP Authorisations (Standalone) holders[8]
- 31 ILDOs (Standalone ILD and UL ILD), and 8 UL(ILD) authorisation holders[9]
- 51 NLDOs (Standalone NLD and UL NLD), and 14 UL(ILD) authorisation holders[10]

All these licensees across services authorisations follow standard security requirements as prescribed under the licenses. Even the Captive Network licensees (CNPNs) who do not connect with any public networks adhere to license security conditions. **It is difficult to understand**

[6] https://dot.gov.in/sites/default/files/List%20of%20UL%20ISP%20license%20as%20on%2031-05-2024.pdf?download=1
[7] https://dot.gov.in/sites/default/files/List%20of%20UL%20VNO%20ISP%20license%20as%20on%2031-05-2024.pdf?download=1
[8] https://dot.gov.in/sites/default/files/List%20of%20Standalone%20ISP%20license%20as%20on%2031-05-2024.pdf?download=1
[9] https://dot.gov.in/sites/default/files/List%20of%20ILD%20Licensees.pdf?download=1
[10] https://dot.gov.in/sites/default/files/List%20of%20NLD%20Licensees.pdf?download=1

therefore why unlicensed M2MSPs offering critical M2M/IoT services using unlicensed spectrum do not fall under its purview.

In contrast, the M2M Service Providers and WPAN/WLAN Connectivity Providers for M2M Services (collectively referred to as **"M2MSPs"**), even though operating large-scale telecommunication networks connected to public resources and providing various critical services, are kept out of these security requirements despite using license-exempt spectrum to provide a variety of services — including tracing, tracking and data acquisition services via low power, short range radio frequency devices such as wireless sensors and actuators, smart meters, wireless industrial applications, wideband data transmission systems, location systems, wireless control systems, etc.

Further, to provide these services, M2MSPs use antennae, wireless carriers, signalling schemes and also various network protocols including IP – similar to licensed TSPs. This should also be looked at from the angle of cybersecurity threats. There have been multiple incidents of cyber-attacks in recent years – at both the national and international levels.

In view of the facts presented above, that all licensees as highlighted above are subject to security requirements; to mitigate increasing cyber security threats, Airtel recommends that:

1. **All M2M devices to be used for critical M2M/IoT services in India should be brought under the NSDTS framework.**

Q4. Whether there is a need for establishing a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs? If yes, –

(a) What should be the saliant features of such a framework?
(b) In which scenarios, the transfer of ownership of M2M SIMs should be permitted?
(c) What measures should be taken to avoid any misuse of this facility?
(d) What flexibility should be given to a new M2MSP for providing connectivity to the existing customers?

Please provide a detailed response with justifications.

Airtel Response:

Yes, a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs should be established. The process of transfer of ownership of M2M SIMs should be kept as simple as possible. This will enhance Ease of Doing business.

Before prescribing the saliant features of such a framework, here is a list of the scenarios in which ownership transfer of M2M SIMs should be allowed.

(b) The scenarios in which transfer of ownership of M2M SIMs should be permitted:

i. Mergers, acquisitions, hive off/split, takeover of companies
ii. Transfer of ownership from the parent company to its subsidiaries/other group companies or vice versa, or between the subsidiaries/group companies of a single parent company
iii. Cessation of operations or filing for bankruptcy by M2MSP
iv. Change of System Integrators (SI) by principal entities (for example, DISCOMs changing contracts from one SI to another or wanting to own the SIMs at a later stage)
v. Business continuity in case of partnerships when some partners become unviable.

Transfer of ownership should be allowed between inter-circle and intra-circle entities.

(a) Saliant features of such a framework:

The process of transfer of ownership of M2M SIMs should be kept as simple as possible to ensure that this can be concluded seamlessly without any customer impact. **The framework should only prescribe the scenarios in which such transfers may be undertaken seamlessly,** i.e., KYC of the new entity with *No Objection Certificate* (NoC) of ownership from both outgoing and new entities or in cases where the outgoing entity ceases to exist, then the new entity should categorically declare the same. The decision of NoC should be left to the TSP due to dynamic market conditions**.** The format of the NoC may be suggested by the DoT.

The other terms and conditions, including the SLAs and inter-se obligations between the transferor and the transferee, should be left to mutual agreement between parties.

Since the physical SIMs are installed in extended geographies, there should be no requirement of issuance of new SIMs or deactivation/reactivation. The transferred SIMs should be allowed to continue with the earlier configuration parameters, so that the transfer may be undertaken without rebooting IoT devices. This is essential to prevent any disruption to services (especially, critical services being provided through M2M SIMs) and to protect the interests of the consumers.

(c) Measures to be taken to avoid any misuse of this facility:

As M2M SIMs offer limited services, potential misuse as a scenario does not exist. However, still the KYC process elaborated above should suffice in cases where prior to bulk transfer of M2M SIMs from one M2MSP to another, the details of the transferee M2MSP, along with an NOC conveying concurrence of both the transferor and the transferee, should be provided to the TSP/Licensee by the transferor M2MSP.

Post the transfer, the transferee M2MSP should comply with the KYC requirements. It should maintain a database of the details of end custodians and keep the same updated.

(d) What flexibility should be given to a new M2MSP for providing connectivity to the existing customers?

Since physical SIMs are installed at extended geographies, there should be no requirement of change of SIM.

Further, in case of transfer of ownership between one legal entity to another, the 'End Custodian' details as prescribed by M2M Guidelines 2018 available with the TSPs should be transferred as well i.e. from a TSP standpoint the details stored in the database against the first M2MSP would be transferred to the new M2MSP.

Q5. Whether there are any other relevant issues relating to M2M/IoT services sector which require to be addressed at this stage? Please provide a detailed response with justifications.

Airtel Response:

It is important to highlight that the RF Mesh technology is used to provide various M2M services today, for instance Advance Metering Infrastructure (AMI) deployments. While services using Low Power Wide Area Network (LPWAN) technology can only be provided by Unified Licensees (Access/M2M authorisation), there is no such mandate on RF Mesh – even though LPWAN and RF Mesh are technological equivalents. This leads to a non-level playing field between services provided by licensed TSPs using LPWAN and those provided by unlicensed operators through RF Mesh. This issue is discussed in detail in the remainder of this response.

Similarities between LPWAN and RF Mesh:

RF Mesh follows almost identical architecture to Low Power Wide Area Networks (LPWAN) networks, except that RF Mesh is based on mesh topology in which each network element acts like a repeater. This way, each element can be accessed directly from an access point or via another network terminal element through one or several hops. A backhaul could be provided using ethernet or cellular technologies etc. The basic RF Mesh architecture is given below:

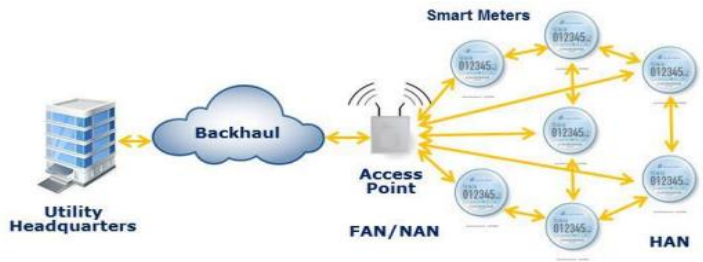

Figure: Basic RF Mesh Network Topology

In India, both LPWAN and RF Mesh technologies use the spectrum portfolio (operate in the same spectrum band, i.e., 865-868 MHz) and are built to have the same performance characteristics. Thus, the area covered through both the technologies tends to be very similar. Further, RF Mesh may scale up to a large WAN – spanning over large geographies like entire cities or districts or even states – through interconnection of multiple WLANs. Thus, networks like AMI, deployed using RF Mesh technology across large areas like entire cities or beyond, cannot be termed as personal/local area networks but rather are equivalent to wide area networks.

Similar to LPWAN, these RF Mesh networks also consist of low power devices like smart meters. Clearly, since technologies used by various unlicensed M2M/IoT service providers in many cases cover wide areas (i.e., cities, districts or even States) and connect devices at scale (e.g., smart meters etc.) - making them equivalent to LPWAN - which itself is a licensed service under the M2M authorization of Unified License – will ensure level playing field is maintained in the area.

Non-Level Playing Field Issues & Risk of Disruption of Public Utility Services:

Despite offering similar services as pointed out, licensed operators using LPWAN are subject to strict compliance requirements under the license, whereas unlicensed operators using RF Mesh are given a free run. The technologies used by various unlicensed M2M/IoT service providers in many cases cover wide areas (i.e., cities, districts or even States) and connect devices at scale (e.g., smart meters etc.), making them equivalent to LPWAN, itself a licensed service under M2M authorization of Unified License.

The issues of a non-level playing field for licensed operators vis. a vis. unlicensed player who neither pay any regulatory fee/levy nor pay auctioned price for spectrum nor fall under ambit of any compliance requirements, and risks to public utility infrastructure and the lack of mitigation measures as suggested in the response to Q2 - are equally applicable in the case of RF Mesh which is presently not within the regulatory ambit.

In the absence of a holistic framework, the risk of disruption or degradation of services can become more pronounced as the footprint of RF Mesh networks like AMI increases.

Therefore, Airtel recommends that:

1. **RF Mesh technology should be treated at par with LPWAN for M2M services and, consequently, be brought within the ambit of regulation immediately. It should be mandated to be provided only by licensed operators and only through licensed spectrum.**

ANNEXURE – A

Indicative list of services / segments to be brought under critical M2M/IoT services:

i. Connected vehicles and autonomous cars/three wheelers and two wheelers along with ***Battery Management System****
ii. Mission critical remote surgery and other health related applications
iii. Trauma and burn patients handling and care leading to National Injury Surveillance
iv. Remote patient tracking and monitoring (home/in-patient)
v. Remote diagnostics
vi. Drug management
vii. Remote control in mining, oil & gas and critical infrastructure construction projects
viii. Safety & surveillance; state, commercial and home security monitoring; surveillance applications, fire alarm, Police
ix. Defence networks
x. Financial transactions
xi. Remote early warning sensors – for weather alert and disaster management
xii. Energy Smart Grids
xiii. Utilities distribution networks including power, water and cooking gas
xiv. Smart meters for energy, water, gas and other such utility services*
xv. Distribution network of inflammable/explosive articles
xvi. Chemical and nuclear industry
xvii. Food industry including smart cultivation, storage and Public Distribution Systems
xviii. Aviation – remote radar systems
xix. Drone communications including UAV-UAV, UAV-GCS and UAV-Network
xx. Space and research
xxi. Control network of Smart Cities
xxii. Smart streetlights, poles*
xxiii. Smart solar panels
xxiv. Industrial machineries in Smart Factories/Industry 4.0*
xxv. Robotics*

**** The highlighted and emboldened text is additionally suggested by industry.*** *Rest is as suggested by IMWG*