COAI counter comments to Consultation Paper on Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs

---

We thank the Authority for providing us with the opportunity to share the counter comments to this Consultation Paper on "Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs".

1. ***One of the stakeholders has stated "there is no need of dividing M2M/IoT services into critical and Noncritical category."***

COAI Counter Comments

a. We strongly oppose the statement mentioned above for the requirement to not identify Critical Services in M2M/IoT sector. M2M sector represents a future where billions to trillions of everyday objects, along with the surrounding environment would be connected through networks, devices and cloud-based servers. It is a well-known fact that some of these sectors are of critical importance to the nation.

b. To deliberate on these issues and arrive at a conclusion, TRAI had issued a Consultation Paper on "Spectrum, Roaming, and QoS related requirements in Machine-to-Machine (M2M) Communications" dated 18th October 2016. Based on inputs provided by all the stakeholders, deliberations and Open House Discussion (OHD), TRAI issued the Recommendations on 05th September 2017. In the same, TRAI stated "*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*."

c. **Government of India accepted TRAI Recommendations after a gap of three years which was promulgated vide DoT letter No. 4-16/2015-NT dated 02nd March 2020.** The Government formed an Inter-ministerial Working Group (IMWG) in November 2019 to understand the sectoral requirements of Critical M2M Services. In March 2021, the IMWG released its report wherein it identified twenty separate M2M services as "critical".

d. Subsequently, DoT in its letter no. 4-31/M2MCriticalServices/2019-NT dated 22nd March 2023 further differentiated between *critical* and *non-critical* services in the M2M/IoT ecosystem. Whilst observing that *"A large number of devices and applications in M2M/IoT ecosystem will be noncritical in nature"*, DoT has affirmed that the *critical* services are to be mandatorily provided through connectivity providers using licensed spectrum. **Only these critical services are yet to be approved by the DoT as referred to in Para 1.16 of the present Consultation Paper.**

e. Thus, the need for critical M2M services is already well established and there is no need to revisit the already accepted Recommendations issued by the Authority mandating that Critical M2M Services should be provided on Licensed Spectrum Band.

2. ***Some of the stakeholders have stated "there should not be any mandate to provide critical M2M services only through the licensed telecom operator over licensed spectrum" and "enforcing the provision of critical services through Licensed bands only by Licensed TSPs may hamper the growth of the market as well as market driven R&D /startups/ smaller companies."***

   Some other stakeholders have also stated that "due to unique features of LPWAN and LoRaWAN technology (low power requirements and long range), various useful M2M/IOT solutions can be developed, which would play vital role in strengthening the overall M2M / IoT ecosystem in India including critical services. Hence, TRAI is requested to kindly review its earlier recommendation of only using licensed spectrum for critical M2M services"

   COAI Counter Comments

   a. It must be noted that the Government has administrative control over the licensed connectivity providers. Also, in case of the Licensed TSPs, the QoS parameters are measurable and enforceable. Moreover, TSPs have to comply with the National Security Directive on telecom and are also subject to the regulations and guidelines framed by TRAI and DoT, pertaining to security, quality of service, etc. Additionally, the internet traffic over the licensed spectrum bands is subjected to continuous monitoring for response to resolution and management of any crisis regarding cyber security in telecom sector.

   b. In contrast, devices and applications using unlicensed spectrum have limited security built for data and signaling equipment as also the traffic generated by the devices and applications using the unlicensed spectrum are not put through any of this rigorous testing, monitoring, and compliance framework. This makes these systems much more prone to vulnerabilities, threats and cyber-intrusions and can even lead to disruption in operations of critical public infrastructure.

   c. We further submit that **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**.

   d. Further, use of low power equipment in the license-exempt band without any safeguard or protection, could face interference from out-of-band or spurious emissions. This can cause performance degradation in the license-exempt band, thereby leading to potential disruption of critical public infrastructure and even National Security.

   e. Moreover, unlicensed spectrum is not exclusively owned, which implies that there is no central agency which could manage the effective use of this spectrum, there is a need to manage interference (to support unlicensed mode) which undermines the advantages of the low-frequency spectrum.

   f. As stated above, in order to deliberate on these issues, TRAI had issued a Consultation Paper on "Spectrum, Roaming, and QoS related requirements in Machine-to-Machine (M2M) Communications" dated 18th October 2016. Based on inputs provided by all the stakeholders, deliberations and Open House Discussion (OHD), **TRAI issued the Recommendations on 05th September 2017. In the same, TRAI stated "*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 Government accepted the TRAI Recommendations and constituted IMWG to identify Critical M2M services.**

g. DoT vide its letter no. 4-31/M2MCriticalServices/2019-NT dated 22nd March 2023 invited comments for finalizing critical M2M services. Whilst observing that *"A large number of devices and applications in M2M/IoT ecosystem will be noncritical in nature"*, DoT has affirmed that the *critical* services are to be mandatorily provided through connectivity providers using licensed spectrum.

h. In light of the above, we submit that it is now well recognized that critical services would require *"robust, resilient, reliable, redundant and secure networks"* as well as *"ultra-reliability, very high availability and accountability"* and therefore, **these services should be provided mandatorily on connectivity using the licensed spectrum bands.**

i. Hence, there is no need to revisit the already accepted Recommendations issued by the Authority mandating that Critical M2M Services should be provided on Licensed Spectrum Band.

3. One of the stakeholders has stated "the requirement of approval from NSCS shall not be applicable to M2M devices."

COAI Counter Comments

a. We disagree with the statement that the requirement of approval from NSCS should not be applicable to M2M devices.

b. The telecom network/infrastructure is deployed on the principles of zero trust and the licensed Telcos are obliged to incorporate all contemporary communication security related elements while procuring the equipment and deploying the same in their network. DoT or its designated agencies have the liberty to inspect all elements, equipment, software etc. procured and implemented by Telcos at any time.

c. Moreover, licensed Telcos are also required to notify DoT on a regular basis for the changes and upgrades in their software. Even when licensed Telcos acquire communication devices which operate using unlicensed spectrum, such as Wi-Fi routers, GPON devices etc. they have to comply with the restrictions pertaining to Trusted Sources under NSDTS. In fact, Captive Non-Public Network (CNPN) licensees, which are not allowed to connect to any public telecom network, are required to comply with these restrictions as well.

d. Whereas the unlicensed entities operating on a large-scale telecommunication network and connected to public resources in this country are not required to comply with any of the security obligations. Since these devices are working on license exempt spectrum, the traffic generated by them does not go through any proper testing, monitoring and compliance procedure. This makes them vulnerable compared to systems using licensed spectrum.

e. Since these devices work on unlicensed spectrum or non-radio equipment and equipment with limited or no security, external persons or agencies may get central

access to the control centre as well as databases required for the operation of the connected public utility infrastructure with the intent to harm.

f. Apart from their working on unlicensed spectrum, the devices are not necessarily procured from 'Trusted Sources' and the operations in license-exempt band are not governed by 3GPP or any other standardization body, nor by any spectrum harmonization rules. Utilizing such license-exempt bands can lead to wide scale proprietary implementations, causing harmful interference to the adjacent licensed band operations.

g. Proliferation of such unlicensed telecom networks in the absence of proper security framework in place, does not bode well for the wider cross-sectoral business ecosystem as well as for national security. **In order to prevent significant security breaches in crucial telecommunications infrastructure and to protect national security, the same security responsibilities should be imposed on these systems as well if license-exempt frequency bands are permitted for the deployment of similar networks and delivery of similar services.**

h. Therefore, we strongly oppose the statement made above and **reiterate the requirement of mandating the procurement of devices and network equipment from only "Trusted sources" designated by National Security Council Secretariat (NSCS) applicable to M2M devices which are to be used in India for critical M2M services.**

----XXX----