COAI Response to TRAI CP on the Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIM

---

1. At the outset, we would like to thank the authority for providing us with the opportunity to respond to the Consultation Paper. The M2M Services have become critical across various sectors such as utilities, power (Smart Meters), finance (Point of Sale), transportation (Connected Vehicles, Battery Management Systems), strategic entities (Space, Defence), manufacturing, healthcare (Telemedicine), etc., catering to critical systems of the country.

2. To address the issues related to M2M Services, TRAI had issued a Consultation Paper on "Spectrum, Roaming, and QoS related requirements in Machine-to-Machine (M2M) Communications" dated 18th October 2016 seeking inputs from members on the issues pertaining to the consultation paper. There were detailed deliberations which involved the inputs of all stakeholders, and an Open House Discussion (OHD) was held by TRAI. **During the Consultation process, COAI had submitted with detailed justification that critical M2M services should be permitted to be provided only on licensed spectrum bands by Licensed Service Provider.**

3. 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*."

4. **It is pertinent to note that 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.**

5. As critical services in M2M sector were left to be identified by DoT, 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". **Only these critical services are yet to be approved by the DoT as referred to in Para 1.16 of the present Consultation Paper.**

6. It is pertinent to highlight that due to this long-drawn process, which is now nearly eight years long, a large no. of M2M Service Providers have already started providing services which may fall in the category of Critical M2M Service in the unlicenced band, which will have major ramifications with regard to safety of our citizen and the security of the country.

7. **COAI reiterates its position, vide its response to TRAI CP on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" dated 12th January 2017 stating that critical M2M services should be provided on license Spectrum Band which was accepted by the Government in March 2020.**

8. In light of the above, we submit that 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.

With regard to the issues mentioned in the present Consultation Paper, **we make our submissions as follows which is inter-alia a re-iteration of our earlier submission made in the year 2017:**

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.

COAI Response

1. We submit that there is a need for a broad guiding framework which would define a service as critical M2M/IoT service based on its importance to national security, public well-being and benefit to the Government at large. Such a framework would ensure consistency across various industries, comprehensive coverage, better resource allocation, effective risk management, etc.

2. With regard to broad guiding framework, we submit that the following can be considered for defining a service as a critical M2M/IoT services:

    a. **Vital to National Interest:** Services supporting critical business operations and infrastructure which are vital to national interests. These services ensure the continuous functioning of the critical infrastructure, thereby safeguarding national security and public welfare.

    b. **Revenue loss to the Government:** Services whose disruption can lead to severe consequences such as interruption of services and significant revenue losses for the Government.

    c. **Importance to National Security:** Refers to any Service provider assisting or supporting the running of Critical infrastructure in the country. Disruption of these services can result in threat to the national security.

    d. **Safety concerns with regard to citizens:** Services which can cause health, safety and environment hazards to citizens of the nation. Their malfunction could potentially endanger public well-being as well as damage the ecosystem of the country.

3. **Standards and inter-operable systems:** Further, for ensuring reliability and redundancy in the Critical M2M/IoT architecture and devices, it is important that it is based on standards and inter-operable systems.

4. Therefore, considering the above, we submit that these factors should be taken into consideration while formulating the framework for defining a service as Critical M2M Service.

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.

COAI Response

1. We submit that there is no need to review the TRAI recommendations dated 05.09.2017. These recommendations were formulated after thorough deliberations and input from all stakeholders.

2. We disagree with the DoT's reference to TRAI justifying the use of unlicensed bands, arguing that many start-ups are designing their models for license-free bands and that enforcing the use of licensed spectrum would hamper market growth. While services and apps may be categorized as start-ups, a pan-India or LSA-wise telecom infrastructure for supporting M2M services cannot be classified as a start-up. Further, any startup providing Critical M2M services as per the guiding framework listed in response to question 1 above will fall under the scope of critical M2M service and the same should be offered on licence spectrum band.

3. Moreover, any entity wanting to provide telecom services must obtain a license. If start-ups establish a wide area network (WAN) for critical M2M services, it is equivalent to telecom services provided by licensed telcos, requiring the same regulatory oversight and standards.

4. Similarly, we submit that the justification of use cases given by DoT while sending the reference to TRAI is not relevant. Segregating various use cases in a particular sector as critical and non-critical will be very cumbersome and time consuming. It is pertinent to note that allowing ministries/ regulatory bodies to independently determine criticality based on market requirements may lead to inconsistencies, gaps in national security and public safety. Thus, a holistic sectoral approach should be adopted.

5. It is imperative to note that DoT accepted TRAI's Recommendation dated 05th September 2017. Subsequently, an Inter-Ministerial Working Group (IMWG) was formed comprising of various ministries in order to define critical services based on the regulatory requirements of the respective ministries. Based on the deliberations, the IMWG identified a list of twenty services as *Critical Services* in the M2M sector.

6. Further, it must be noted that 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.

7. On the contrast, devices and applications using unlicensed spectrum have limited security built for data and signalling 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.

8. 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.

9. In light of the above, we submit 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.

10. The suggestion that some of the services in critical sectors can be offered on unlicensed spectrum would undermine and impact the entire infrastructure, leading to isolated silos of connectivity, duplication of capex across interconnected sectors, and would affect the entire flexibility, security and scalability that planners require in these critical services sectors.

11. It is also apropos to note that allowing critical services in the M2M sector using unlicensed spectrum introduces significant risks related to reliability, security, regulatory compliance, and overall service quality. The risks are illustrated below in detail:

i. <u>Lack of security checks for license-exempt spectrum:</u>

a. Devices and networks using license-exempt spectrum have limited security built for data and signalling in contrast with the equipment deployed by licensed TSPs. Also, the regulations and guidelines framed by TRAI and DoT, pertaining to security and quality of service are applicable only for the usage of licensed spectrum bands.

b. The traffic generated by devices using the license-exempt spectrum are not put through any proper testing, monitoring and compliance procedure. Thus, devices using license-exempt band are already more vulnerable compared to the systems using licensed spectrum, due to lack of proper regulations and appropriate security checks.

c. On top of that, the lack of testing and monitoring will make these systems much more prone to vulnerabilities, threats and cyber-intrusions.

ii. <u>Disruption in operations of public infrastructure:</u>

a. As this infrastructure will rely on license-exempt 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.

b. On the other hand, as these systems do not have stringent compliance or monitoring requirements, human errors or internal incidents can also result in such failure along with major accountability issues.

c. 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.

iii. <u>Interference to operations of licensed TSPs:</u>

a. As 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, neither 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.

iv. <u>Central agency:</u>

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.

12. Hence in light of the above, we submit that there is no reason to revisit Para 5.1(g) of the TRAI Recommendation which states that Critical M2M Services should be provided on Licensed Spectrum Band.

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.

<u>COAI Response:</u>

1. We submit that **all M2M devices which are to be used in India for critical M2M should be brought under the Trusted Source / Trusted Product Framework.**

2. 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 the Telcos at any time. The licensed Telcos are also required to notify DoT on regular basis for the changes and upgrades in their software.

3. Even when the 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. Whereas, ironically, unlicensed entities, which are operating large-scale telecommunication networks and connected to public resources in this country are not required to comply to any of the security obligations, thus posing significant threat to the National Security.

4. We would like to further highlight the comparison of the obligations of Telcos using licensed spectrum and operators using licensed-exempt spectrum as under. The issues of a non-level playing field are evident from the table below:

S No.	**Area of Regulation**	**Telecom Service Providers**	**Operators license-exempt spectrum**
1.	Spectrum allotment and use	Need to bear high spectrum acquisition cost.	No such costs.
2.	License Fee	Pay the License Fee.	No such costs.
3.	Spectrum related charges	Pay Spectrum Usage Charges.	No such costs.
4.	Quality of Service Parameters	Need to comply as part of regulatory regime.	No such requirement.
5.	All security conditions	Need to adhere to all rules.	No such requirement.
6.	Monitoring services i.e Lawful interception and Monitoring	Need to comply as part of the license condition.	No such requirement.

5. We further submit that all licensed Telcos are directed to store the IPDR/CDR for all communication exchanged through the deployed systems. On the contrary, there is no obligation on the unlicensed operators for such storage of date.

6. In addition, Internet Monitoring System (IMS) & IPFIX probes are used to analyse the internet traffic of licensed Telcos in order to respond to, manage, and address any cyber security related crisis in the telecom sector. Additionally, the licensed Telcos face harsh financial penalties for non-compliance and even inadvertent errors.

7. **On the contrary, unlicensed companies operating inside the telecom ecosystem that are offering a variety of services using license exempt**

spectrum and are NOT subject to the National Security Directive on the Telecommunication Sector (NSDTS). These include data collecting, tracing, and tracking services using low-power, short-range radio frequency devices such as wireless sensors and actuators, smart metres, wireless industrial applications, wideband data transmission systems, location systems, wireless control systems, etc.

8. Antennas, wireless carriers, signalling protocols, as well as other network protocols, including IP, are required for the delivery of such services. These components are also necessary for the telecom operations carried out by licensed Telcos. Fundamentally, whether these services are offered by an unlicensed entity or a licensed Telcos, the technology requirements for supplying them remain the same. In a similar way as licenced Telcos, unlicensed companies are thus offering services that are similar to telecommunication services**. However, the unlicensed entities are not subjected to any of the security obligations applicable for licensed Telcos, as elaborated above.**

9. **Thus, in light of the above, we submit that all M2M devices which are to be used in India for critical M2M should be brought under the Trusted Source / Trusted Product 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 salient 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.

COAI Response:

1. We submit that the transfer of ownership of M2M SIMs should be allowed between companies.

2. The process of transfer of ownership of M2M SIMs should be kept as simple as possible in order to ensure ease of doing business (EoDB) for the players in the M2M ecosystem. Moreover, the customers want the ownership transfer to happen without any service disruptions. Given that M2M SIMs are used for various critical services, and embedded SIMs are being used exceedingly in this sector, there is a need for explicit guidelines for efficient transfer of ownership of M2M SIMs.

3. The need for transfer of M2M SIMs will arise in the following scenarios:

   a. involving merger, acquisitions, hive off/split, takeover of companies.

b. for cases wherein companies wish to transfer the ownership from the parent company to its subsidiaries/ other group companies or vice versa/ and between its subsidiaries/ group companies.

c. for cases wherein M2M service provider is ceasing its operations or is filing for bankruptcy, etc. and the M2M SIMs are required to be either transferred to the new M2M service provider or directly to the company where M2M SIMs are used/ deployed.

d. 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)

e. Business continuity in case of partnerships when some partners become unviable.

f. There could be various scenarios on the field which may require transfer of ownership of M2M SIMs. For example, a DISCOM may give a tender to any entity for a certain period and at the end of expiry of the tender, a new entity could get the tender. All such scenarios need to be catered to.

4. For the purpose of all these transfer of / change in ownerships scenarios, all the M2M SIMs (i.e. the 13-digit SIMs as well as M2M SIMs issued prior to issuance of 2018 DoT guidelines) owned by the entities shall be covered.

5. In all the scenarios listed above, all the terms and conditions pertaining to transfer of M2M SIMs should be mutually agreed upon, including the SLAs and obligations, between the two entities which are involved in the transfer process. The mutual agreement between the two entities may be driven by market forces. We do not see any need of regulatory intervention.

6. In all the scenarios listed above, the entity which is acquiring the M2M SIMs may take a No Objection Certificate (NOC) for providing service to acquired M2M SIMs, from the entity which is transferring the ownership of M2M SIMs.

7. In HQ-to-HQ transfer i.e., where existing M2M setup of a customer is taken over by another customer e.g., in case of merger or takeover of companies, M2M service provider should be allowed to handle the transfer in such a way that IoT device reboot should not be required, and M2M SIMs can continue with earlier configuration parameters. Thus, in such cases only the date of transfer along with new organisation details are to be updated and subscription should not be forced to go through detach and attach activity as it may result in M2M device going offline.

8. Transfer of ownership should be allowed seamlessly across LSAs.

9. In case of transfer of ownership of M2M SIMs, the M2M service provider which is transferring the ownership of SIMs will be responsible for intimating the TSP/ Licensees the details of the entity/M2M service provider to whom such M2M SIMs/devices are transferred.

10. The responsibility for fulfilling the subscriber verification norms lies with the entity/organization providing M2M Services i.e., the entity/organization which has acquired such SIMs because of the transfer of ownership. The end-custodian details should be available with the M2M service provider. The M2M service provider shall regularly update all the necessary details in their database.

11. 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.

12. We further submit that there should be no requirement of recording the data pertaining to the transfer of ownership on the Saral Sanchar portal. Currently, there is no practice of uploading information pertaining to the M2M service providers to the Saral Sanchar portal and hence there is no reason for doing the same in the case of transfer of ownership cases as well. We submit that this practice should be continued with. Such data shall be available with the concerned M2M service provider who is acquiring the M2M SIMs by virtue of transfer of ownership.

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.

COAI Response:

1. Include RF Mesh as LPWAN and bring under Unified License Services

   a. By integrating multiple RF Mesh Networks (WPAN/WLAN), the RF Mesh service providers are creating large city or State-wise WAN. These unlicensed entities utilize Antennas, wireless carriers, signaling protocols, as well as other network protocols, including IP, for the delivery of such services. These components are also necessary for the telecom operations carried out by licensed TSPs.

   b. Fundamentally, whether these services are offered by an unlicensed entity or a licensed TSP, the technology requirements for supplying them remain the same. In a similar way as licensed TSPs, unlicensed companies are thus offering services that are similar to telecommunication services.

   c. In view of the similarities between RF Mesh and LoRaWAN (LPWAN) as well as to ensure level playing field between entities providing similar services, **we request the Authority to recommend bringing the RF Mesh technology at par with the LPWAN technologies for M2M services and also bring RF Mesh service providers under the ambit of the M2M authorization of Unified License. RF Mesh players also need to be brought under the framework of MTCTE and NSDTS.**

------XXX------