RJIL/TRAI/2024-25/137
19th August 2024

To,
Shri Akhilesh Kumar Trivedi,
Advisor (Networks, Spectrum and Licensing),
Telecom Regulatory Authority of India,
Tower-F, World Trade Centre,
Nauroji Nagar, New Delhi - 110029

Subject: **RJIL's comments on TRAI's Consultation Paper on "Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs".**

Dear Sir,

Please find enclosed the comments of Reliance Jio Infocomm Limited (RJIL) on the Consultation Paper dated 24.06.2024 on **"Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs"**.

Thanking you,

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

KAPOOR SINGH GULIANI
Digitally signed by KAPOOR SINGH GULIANI
Date: 2024.08.19 16:43:05 +05'30'

Kapoor Singh Guliani
Authorized Signatory

Enclosure: As above

Reliance Jio Infocomm Limited's comments on TRAI's Consultation Paper on the Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs dated 24th June, 2024

Preface

1. At the outset, we thank the authority for issuing this consultation paper relating to crucial issues pertaining to the administration of critical IoT/M2M services on the reference of the Department of Telecommunications.

2. Per numerous reports from analysts and researchers across the globe, the IoT market is growing rapidly, at around 20% year on year by some estimates. Some also estimate the sector to grow to over USD 2 trillion by the end of the decade[1] [2] [3]. The rapid growth of IoT is due in large part to its ability to transform and revolutionize various sectors such healthcare, transportation and Industry 4.0.

3. As highlighted by the Authority in its consultation paper, an Inter-Ministerial Working Group (IWG) was constituted in November 2019 to identify Critical Services in the M2M sector. As per the extracts from the committees report, shared by TRAI in the consultation paper (Annexure I), critical IoT differs from Massive IoT as it requires ***"high QoS, ultra-reliability, very low latency, very high availability along with accountability with requisite security"***

4. The Inter-Ministerial Working Group also recommended that the following services be defined as Critical M2M/IoT services

    i. *Connected and Autonomous Cars*
    ii. *Remote Surgery*
    iii. *Trauma and Burn Patients Handling*
    iv. *Remote Patient Monitoring & Tracking*
    v. *Remote Diagnostics*
    vi. *Drug Management*
    vii. *Remote Control in Mining, and Oil & Gas*
    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*

---

[1] Mordor Intelligence, 2024. *IoT Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029).* [Online] Available at: https://www.mordorintelligence.com/industry-reports/internet-of-things-iot-market [Accessed 17 July 2024].

[2] SkyQuest Technology Group, 2024. *Internet Of Things (IoT) Market Size, Share, Growth Analysis, Industry Forecast 2024-2031.* [Online] Available at: https://www.skyquestt.com/report/internet-of-things-market [Accessed 17 July 2024].

[3] Allied Market Research, 2024. *Internet of Things (IoT) Market Size | Industry Report - 2030.* [Online] Available at: https://www.alliedmarketresearch.com/internet-of-things-IoT-market [Accessed 17 July 2024].

xiv. *Distribution network of inflammable/explosive articles*
xv. *Chemical and Nuclear Industry*
xvi. *Food Industry including Smart Cultivation, storage and public distribution*
xvii. *Aviation – Remote Radar Systems*
xviii. *Drone Communications including UAV-UAV, UAV-GCS, and UAV-Network*
xix. *Space & Research*
xx. *Control Network of Smart Cities*

RELEVANCE AND IMPACT OF CRITICAL IOT SERVICES

5. Critical IoT services, as defined by the Inter-Ministerial Working Group, require high levels of reliability and low latency for time-sensitive applications and use-cases. These services will play a crucial role in enhancing public safety, healthcare, industrial productivity, and urban mobility.

6. In emergency response scenarios, IoT devices would help provide real-time data to first responders, and allow them to make quick and informed decisions. High levels of reliability and low latency for such services would ensure that critical information, such as the location of individuals in distress or the status of infrastructure is delivered quickly and efficiently.

7. In the healthcare sector, the critical IoT services highlighted by the Inter-Ministerial Working Group will enable real-time monitoring and treatment of patients, including for those with chronic conditions or in intensive care units. Healthcare IoT devices will continuously monitor vital signs and immediately alert healthcare providers to any abnormalities for timely intervention. Guaranteed low latency and reliable data transmission are vital network performance indicators in such settings, where delays can lead to adverse health outcomes. The critical IoT healthcare services highlighted by the IWG also support telemedicine, remote diagnostics and treatment, which are of great relevance in rural or underserved areas across the nation.

8. Industry will also significantly benefit from critical IoT services. In smart manufacturing/Industry 4.0, IoT devices will monitor and control machinery to guarantee optimal performance and prevent malfunctions. Once again, reliable and timely delivery of data in such cases would aid predictive maintenance and increase productivity.

9. The integration of critical IoT services in transportation systems will be key for the development of smart cities. Autonomous vehicles would need low-latency access to navigate safely, and would need to be supported by traffic management systems that use real-time data to optimize traffic flow and enhance urban mobility. Such systems would also need high quality connectivity in order to function as per their intended purpose.

CRITICAL IOT SERVICES SHOULD BE PROVIDED ONLY BY LICENSED TSPs

10. Due to the high performance levels, reliability and security needs of critical IoT/M2M applications and use cases, network access for such services should be provided by licensed TSPs only. This is for the fact that the TSPs only are authorised to use the auctioned spectrum that is free from any interference, due to exclusive use. It is essential to ensure that such

services not only receive the kind of network access they need in terms of reliability and performance, but also to ensure that these are provided by entities that are accountable for performance and security failures and flaws.

11. In its recommendations on 'Spectrum, Roaming and QoS Related Requirements in Machine-to-Machine (M2M) Communications' dated 5th September, 2017, the authority noted the following with respect to the needs of critical IoT applications/use cases

    i. Critical IoT applications require high QoS, ultra-reliability, very low latency, very high availability and accountability, and
    ii. Any variation in QoS, latency or availability of network access for such critical applications can lead to substantial damage for the users of these services.

12. The Authority also recommended that *"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."*** (Emphasis Added)

13. The findings and recommendations of the inter-ministerial working group mirrored the assessment of the Authority. The IWG recommended the following in its report

    i. The critical services should be provided only using connectivity from the licensed telecom operators from DoT.
    ii. These services shall use connectivity being offered on licensed spectrum bands.
    iii. Details regulatory requirements for these critical services shall be issued by respective ministries/ regulatory bodies

14. Licensed spectrum allows for the delivery of high quality M2M services over large areas. Unlike any delicensed spectrum, this spectrum being assigned on exclusive basis, is at minimum risk of interference, and the total capacity can be adjusted dynamically to account for usage. TSPs are already complying with extensive QoS compliances that will ensure that these services receive the level of performance they need for successful deployment and adoption.

15. Based on a comprehensive study of the performance and security needs of critical M2M/IoT services, the Authority and the IWG have both recommended that these services must only be provided by licenced TSPs using licenced spectrum bands. The recommendations by the TRAI and the Inter-Ministerial Working Group are well-considered and thoughtful of the unique performance and security requirements of critical M2M/IoT vis-à-vis massive IoT deployments, and must therefore guide the classification of a service as critical, as well as how these services are to be connected to the public internet.

INCREASING CYBER THREATS ESTABLISH A NEED FOR ACCOUNTABILITY IN THE PROVISIONING OF CRITICAL M2M/IOT SERVICES

16. Cybersecurity incidents and data breaches have been occurring with increasing sophistication and escalating frequency over the last decade. The potential attack surface available to cybercriminals has increased in proportion to both the growth of digital services, and their integration by industry at large. The table below captures some high-profile cybersecurity incidents (with an estimated financial impact of over USD 1 million per incident) over the last one year alone[4].

Month and Year of Reported Breach	Impacted Party	Nature of Compromised Data
May-24	Poland and Czech Republic	Government and infrastructure network data via Microsoft Outlook vulnerability
Apr-24	Russia's United Russia party	Servers, websites, and domains made inaccessible via DDoS attacks
Mar-24	African Union's systems	Over 200 user devices infected, cause unknown
Mar-24	EU members of the Inter-Parliamentary Alliance on China	IP addresses and target locations
Feb-24	Dutch military network	Malware placed, limited damage
Jan-24	Sweden's digital service provider for government services	Operations for 120 government offices disrupted
Jan-24	Kyiv webcams	Camera angles changed to gather information on critical infrastructure
Dec-23	Russia's largest water utility plant	Computers encrypted, data deleted
Dec-23	Ukraine's largest mobile phone provider (Kyivstar)	Customer access disabled, computers and servers destroyed
Nov-23	Philippine government networks	Malicious code to establish command-and-control
Nov-23	Danish power companies	Power grid access targeted via command injection flaw
Nov-23	Cambodian government networks	Disguised data exfiltration as cloud storage services
Oct-23	ASEAN governments and organizations	Espionage software tool
Oct-23	South Korea's shipbuilding sector	Malware phishing for naval intelligence
Sep-23	Israel's railroad network	Phishing campaign targeting electrical infrastructure
Sep-23	US and Japanese government industries	Firmware implants in routers
Sep-23	International Criminal Court	IT systems breached amid war crimes probe

[4] Center for Strategic & International Studies, 2024. *Significant Cyber Incidents.* [Online] Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Accessed 15 July 2024].

Month and Year of Reported Breach	Impacted Party	Nature of Compromised Data
Aug-23	Polish government, rail systems	Rail systems disabled, malicious signal transmitted
Aug-23	US military procurement system	Data exfiltrated via high-bandwidth routers
Aug-23	Ukrainian Armed Forces' combat information systems	Custom malware targeting Android tablets

17. It is clear that the scope and reach of cybercrime is constantly accelerating & evolving, and can have significant ramifications for a country and its people.

18. From smart cities to IoT, the integration of digital technologies creates more opportunities for innovation and efficiency. This expansion of digital services however, also introduces new vulnerabilities for exploitation by cybercriminals. Additionally, the interconnected nature of modern systems also means that a breach in one area can quickly cascade to other sectors and amplify the overall impact.

19. Digital ecosystems continue to become increasingly complex, which makes it more challenging to secure them. It is therefore necessary that such services are provided solely by accountable entities that can respond quickly and effectively to protect data and information flows.

20. Licensed TSPs have set up extensive and ubiquitous networks using licensed spectrum bands, and can guarantee the performance levels required by critical M2M/IoT use cases. Additionally, TSPs have also deployed security policies that will be crucial to protect these services from malicious attacks. **Critical M2M/IoT services should therefore only be provided by licences TSPs.**

ISSUE WISE RESPONSE.

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.

RJIL Response

1. A broad guiding framework for defining a service as a critical M2M/IoT service should include the following considerations

Criteria	Definition	Metrics	Examples
Time Sensitivity and Latency	Services that must operate within stringent time constraints, where delays can lead to significant negative outcomes	Maximum acceptable latency, real-time data processing requirements, and responsiveness under various sector specific operational conditions	Autonomous vehicle navigation, real-time health monitoring, and emergency response systems

Criteria	Definition	Metrics	Examples
Reliability & Availability	Services that require near-constant uptime and resilience to disruptions	Uptime percentage, fault tolerance levels, and disaster recovery capabilities	Utility grid management, critical infrastructure monitoring, and industrial automation systems
Data Integrity & Security	Services that require accurate, secure, and protected data flows	Encryption standards, data validation processes, and adherence to cybersecurity protocols	Financial transaction systems, healthcare information systems, and government communication networks
Safety & Human Impact	Services that can directly affect human health and safety	Potential for harm reduction, emergency intervention capabilities, and compliance with safety regulations	Medical alert systems, disaster warning systems, and hazardous material monitoring
Economic Impact	Services that significantly affect economic activities or operational efficiencies	Cost of downtime, impact on productivity, and potential financial losses.	Supply chain management, automated manufacturing processes, and smart logistics
National Security	Services that are critical to national security, public order, or essential public services	Relevance to national defence, public service continuity, and societal impact	Defence communication networks, public safety systems, and critical public utility management
Scalability & Flexibility	Services that require the ability to scale operations and adapt to increased reach and scope without compromising service quality	Scalability potential, adaptability to new technologies, and integration capabilities with other systems	Smart city infrastructure, nationwide emergency communication systems, and extensive IoT sensor networks

2. We note that the services listed by the inter-ministerial working group as critical IoT services can be determined to be as such using a framework such as the above. We also note that similar considerations likely formed the basis of the assessment of the IWG in its report.

3. The above framework may also be used to classify additional services as critical (such as Smart Meters), as well as for reviewing the criticality of services already defined by the IWG.

4. We submit that there is an urgent need to notify a list critical M2M/IoT services, including Smart Meters. Delays in finalizing what services qualify as critical deprives the National Exchequer of revenue and can potentially lead to complex retrospective regulatory compliances once these are notified.

5. It is pertinent to note that a large number of smart meters have already been sanctioned (~ 225 million) for consumer, transformer and feeder grids by power utilities across the nation. Many of these have also already been awarded to unlicensed Advanced Metering Infrastructure Service Providers (AMISP).

6. Unlike licensed service providers, AMISPs do not have to comply with crucial security protocols such as acquisition of Trusted Products, monitoring under TSOC, mandatory testing etc. The lack of comprehensive security checks & controls renders smart meter deployments by AMISPs at elevated risk of targeting by cybercriminals. The IWG has also recommended

that *Utilities distribution networks including power, water and cooking gas* be defined as a critical M2M/IoT service.

7. We therefore urge the Authority to recommend a framework for defining critical M2M services, as well as recommend that this list be notified with minimum delays.

8. Further, the State Government Authorities are cautioned about the huge security threats in awarding projects to AMISPs.

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.

RJIL Response:

1. No review of the existing recommendations is required. For the reasons mentioned in the preamble above. The recommendations of the Authority with respect to the mandatory provision of these services by service providers with licenced spectrum are even more relevant than when they were first issued in 2017, in view of the increased security threats.

2. Given the performance and security levels required by such services, the prior recommendation of the Authority must guide the development of policies and rules for this purpose.

3. Accordingly, the Authority is requested to reiterate its recommendation on the subject.

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.

RJIL Response:

Due to the need for greater security requirements for critical M2M services, all M2M devices to be used for Critical IoT/M2M services in India 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.

RJIL Response

1. The transfer of M2M SIMs should be permitted under the following conditions.

    i. in the case of mergers and acquisitions among and by registered Indian Companies,
    ii. Among Parent and subsidiary companies, and
    iii. In case an M2MSP is ceasing operations or is filing for the bankruptcy
    iv. Valid Operational requirements 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.

2. Allowing this flexibility is essential to ensure that the subscribers are not inconvenienced and continue to avail M2M services seamlessly and significantly streamline operations in the above cases. Additionally, allowing the transfer of ownership of these SIMs will aid the overall growth of the IoT market due to the fact that this sector is in a nascent stage of deployment, with significant scope for expansion, the introduction of new entrants, and for market consolidation.

3. We feel that by restricting the facility only to above use cases, the Authority can obviate the possibility of any misuse of this facility. Further, permissions can be given on case-to-case basis. However, field operations should have sufficient flexibility to ensure that the operations and customer services are not affected.

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.

RJIL Response

1. Some entities are urging the government to delicence additional frequencies over and above the ISM Band (865-867 MHz) on the grounds that existing allocations are being used by many users and services and causing a high degree of interference. These players are calling for the delicensing of the 915-935 MHz range for use in Critical IoT applications/use cases.

2. We submit that delicensing of frequencies opens them up for use by many entities, exposing them to similar levels of interference. Critical M2M/IoT services are dependent on reliable and available network access, and should therefore be protected from avoidable sources of interference.

3. Therefore, we submit that no additional frequencies need to be delicensed for the above purposes, and in line with our submissions above, all critical M2M/IoT Services must only be provided by licensed TSPs using licenced frequencies.

4. Considering the criticality of M2M services with no relevance with P2P communication, these SIMs should be kept out of the purview of data barring orders issued by all Government authorities.

5. The Authority is requested to recommend for a single CAF for all M2M connections across the country instead of current practice of LSA wise CAFs.