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

The GSMA has been doing extensive work on developing guidelines and designing the appropriate framework for IoT.

In this high- level response, the GSMA would like to make the following key points:

A. Critical services in the M2M sector provided through licensed spectrum

GSMA supports the previous recommendation of the TRAI that critical services in the M2M sector should be mandated to be provided only using licensed spectrum. We would like to highlight some of the key justifications that underscore the importance of licensed spectrum in ensuring the reliability and security of critical IoT services.

1. Reliability and Quality of Service (QoS):

- **Guaranteed Performance**: Licensed spectrum provides exclusive access to operators, which significantly reduces the risk of interference from other users. This exclusivity is crucial for critical applications that require high reliability, low latency, and consistent performance, such as remote healthcare services, autonomous vehicles, and emergency response systems.
- **Measurable QoS Standards**: The use of licensed spectrum allows for the establishment of enforceable QoS standards. Regulatory bodies can set clear performance metrics that must be met by service providers, ensuring that critical services operate within defined parameters that protect end-users.

2. Security Considerations:

- **Enhanced Security**: Critical IoT services often handle sensitive data and require robust security measures. Licensed spectrum provides a more secure environment, as it is less susceptible to unauthorized access and interference compared to unlicensed spectrum. This is particularly important for applications in sectors such as healthcare, finance, and public safety.
- **Regulatory Oversight**: Licensed operators are subject to regulatory oversight, which includes compliance with security standards and protocols. This oversight helps to ensure that critical services are delivered in a secure manner, protecting both the infrastructure and the data being transmitted.

3. Support for Critical Infrastructure:

- **Infrastructure Resilience**: Critical services often rely on a resilient infrastructure that can withstand various challenges, including natural disasters and cyber threats. Licensed spectrum supports the development of robust networks that can provide the necessary redundancy and reliability for critical applications.

- **Long-Term Investment**: The commitment to licensed spectrum encourages long-term investment in network infrastructure by operators. This investment is essential for the continuous improvement and expansion of services that support critical applications.

4. Market Stability and Consumer Confidence:

- **Consumer Trust**: Ensuring that critical services are delivered over licensed spectrum helps to build consumer trust in IoT applications. Users are more likely to adopt and rely on services that are backed by a stable and secure network environment.
- **Market Predictability**: A clear regulatory framework that mandates the use of licensed spectrum for critical services provides predictability for operators and investors, fostering a stable market environment conducive to innovation and growth.

GSMA firmly believes that the recommendation for critical M2M services to be provided exclusively through licensed spectrum is essential for ensuring reliability, security, and quality of service. We urge TRAI to maintain this recommendation to protect the integrity of critical IoT applications and to support the continued growth and development of the M2M ecosystem.

B. IoT Security Guidelines

GSMA has a wealth of security guidelines for the IoT Ecosystem and would recommend TRAI to refer to the following[1]:

1. GSMA IoT Security Guidelines Overview
2. IoT Security Guidelines for Service Ecosystems
3. IoT Security Guidelines for Endpoint Ecosystems
4. IoT Security Guidelines Archive

The **new 2024** revised GSMA IoT Security Guidelines promote best practice for the secure design, development and deployment of IoT services, and providing a mechanism to evaluate

[1] IoT-Guide-Global-IoT-Regulations.pdf (gsma.com)

https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/iot-security/iot-security-guidelines/

CLP.13 v2.2 GSMA IoT Security Guidelines for Endpoint Ecosystems

CLP.12 v2.2 GSMA IoT Security Guidelines for Service Ecosystems security measures. The GSMA IoT Security Guidelines help create a secure IoT market with trusted, reliable services that can scale as the market grows.

The GSMA IoT Security Guidelines:

- Include detailed recommendations for the secure design, development and deployment of IoT services
- Cover networks as well as service and endpoint ecosystems
- Address security challenges, attack models and risk assessments
- Provide worked examples.

C. <u>Other recommendations:</u>

The GSMA recommends a principle-based approach (national interest, economic consequences, health, safety, environmental hazards and standards/interoperable systems) to determine criticality of M2M service. Based on it,, it might be appropriate to include M2M devices in certain critical infrastructure applications.

Furthermore, transferring SIMs between SPs should be done on a case- by -case basis – for example, merger or acquisition, sale of business entity or other aspects where any existing non transferability clause may not be appropriate.

The GSMA would like to thank TRAI for the opportunity to submit its recommendations on this important subject area and we remain available for future engagements as it develops a suitable framework for governance of critical services in the M2M sector.